Development of Electrical Hazard and Probability (ELHAP) Tool Related to Equipment and System Failure

by

Mohd Rosli bin Kamaruddin

Dissertation submitted in partial fulfillment of

the requirements for the

Bachelor of Engineering (Hons)

(Chemical Engineering)

JANUARY 2009

Universiti Teknologi PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

Development of Electrical Hazard and Probability (ELHAP) Tool Related to Equipment and System Failure

by

Mohd Rosli bin Kamaruddin

A project dissertation submitted to the
Chemical Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
BACHELOR OF ENGINEERING (Hons)
(CHEMICAL ENGINEERING)

Approved by,

(A.P Dr. Azmi Mohd. Shariff)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

January 2009

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

MOHD ROSLI BIN KAMARUDDIN

ABSTRACT

Electrical safety in the industrial process plant plays an important role to ensure overall safety of the chemical plant, but most of the time this subject has been largely ignored leading to major accidents in the plant. Due to this reason, many researchers find that it is important to understand completely the electrical system to avoid any accident in the plant. Hazard and Operability (HAZOP) analysis tool is widely used as qualitative tool to identify potential hazards that can cause major accidents in the plant, while the Fault Tree Analysis (FTA) method is widely used to estimate the probability of occurrences of the hazards. However, they have never been implemented vigorously to identify potential hazards due to electrical equipment and system failure. Thus, the main objective of this project is to provide a framework for systematic investigation of the problems in process plant due to electrical equipment and system failure. This project consists of analysis that is done to complement the need for detailed study of the electrical hazard. The analysis will include both qualitative HAZOP analysis approach to identify the possible hazards and a quantitative FTA assessment to rank the hazardous event accordingly for direct implementation in industrial case study. The tools developed will provide a detail review of chemical plant safety focusing on electrical equipments and system design. At the end of the study, the analysis will help to provide suggestion to improve the design, installation, operation and maintenance procedures in order to optimize the safety and operability in the plant.

ACKNOWLEDGEMENT

First and foremost I would like to praise Allah S.W.T The Most Gracious, The Most Merciful for blessing me with the gift of knowledge and health from day one until the completion of the project.

My utmost gratitude goes to my supervisor, A.P Dr. Azmi M. Shariff. He has given precious advice and ideas in completing this project throughout the two semesters. His encouragements and willingness to provide constructive criticism and suggestions are very much appreciated.

I would like to take this opportunity to thank Mr. M. Tazli Azizan, the Final Year Project (FYP) Coordinator for January 2009 for his efforts in making sure that the commencement of FYP is successful. In addition, I would like to express my gratitude to Mr. Zulkifli bin Ibrahim from PETRONAS Fertilizer Kedah Sdn. Bhd., and Dr. Moulay Rachid Babaa as the evaluators for my final oral presentation.

Most important of all, my deepest appreciation goes to my family for their undying love and motivation in seeing me successfully pulls off another great chapter in my life as a student in UTP. Last but not least, I would like to thank my fellow friends for their continuous support and advice in completing this project.

Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	Alternating current
ALARP	As low as reasonably practicable
ETA	Event Tree Analysis
ELHAP	Electrical Hazard and Probability
F&EI	Fire and Explosion Index
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
ICI	Imperial Chemical Industry
IFAL	Instaneous Fractional Annual Loss
OREDA	Offshore Reliabilty Database
OSHA	Occupational Safety and Health Administration
MPPD	Maximum Probable Property Damage
P&ID	Piping and Instrumentation Diagram
PETRONAS	Petroliam National Berhad
PFKSB	PETRONAS Fertilizer Kedah Sendirian Berhad
PHA	Process Hazard Analysis
PTS	PETRONAS Technical Standard
SLD	Single Line Diagram
UPS	Uninterruptible Power Supply

CHAPTER 1
INTRODUCTION

1.1 BACKGROUND OF STUDY

Electrical safety is very critical for any electrical system and equipment operating in the hazardous area such as in the power plant and chemical plant. Hazard and Operability (HAZOP) and Fault Tree Analysis (FTA) tools are the basic components in developing the tool to perform the electrical hazard analysis in this project. The abbreviation for the tool developed will be called **ELHAP** assessment in the entire report. ELHAP is derived from "***Electrical Hazard and Probability***" phrase because the tool not only identifies all of possible hazards, but it provides probability for major hazards. In addition, "*hap*" here also means fortune or luck, in which if it is combined with the "*electrical*" term at the front syllable, it can be interpreted as bringing luck or fortune to the electrical system or to the plant in general since electrical safety analysis is a very crucial element for safe operation in chemical plant.

Detailed study is required to do thorough analysis of the problems due to electrical system and equipment failure. All of the components in the electrical system need to be identified and analyzed from the Piping and Instrumentation Diagram (P&ID) or Single Line Diagram (SLD) of the specific plant. Similar approach to HAZOP method will be used to identify all possible causes of the problems in which a series of guidewords will be introduced as a systematic approach for further analysis. Once the causes are recorded, the safety team involves will list all of the consequences and any recommendation deemed appropriate. During the analysis, if the consequence is very significant in which it involves considerable amount of loss, or major harm to the personnel, FTA tool will be implemented to calculate the probability in order to predict the likelihood of occurrences of the hazard. If the hazard has very high probability, then the recommended actions should be taken into consideration irrespective of cost or changes it will make. Hazard with higher probability must be prioritized to optimize the safety. It is aimed that the tools developed will be used as a practical and systematic framework to analyze and minimize the potential hazards due to electrical equipments and system failure, to ultimately optimize the safety and operability in the plant by improving the system design, installation, operation and maintenance procedures. This is to comply with the safety analysis purpose which is to reduce the risks as low as reasonably practicable (ALARP) in any workplace.

1.2 PROBLEM STATEMENT

HAZOP analysis tool is widely used as qualitative tool to identify potential hazards that can cause major accidents in the plant. However, this tool has never been implemented vigorously to identify potential hazards due to electrical equipment and system failure. In this project, FTA method will be implemented as an additional component along with the HAZOP analysis as the basic component and it will be used as a quantitative tool to rank the hazardous events accordingly. The combination of both methods will provide a newly developed systematic tool to make sure that it is more structured, appropriate and efficient for direct implementation in industrial case study. It is not the intention of this project to duplicate the current tools but it is intended to provide alternative tools for the safety analysis and to complement with the current available tools.

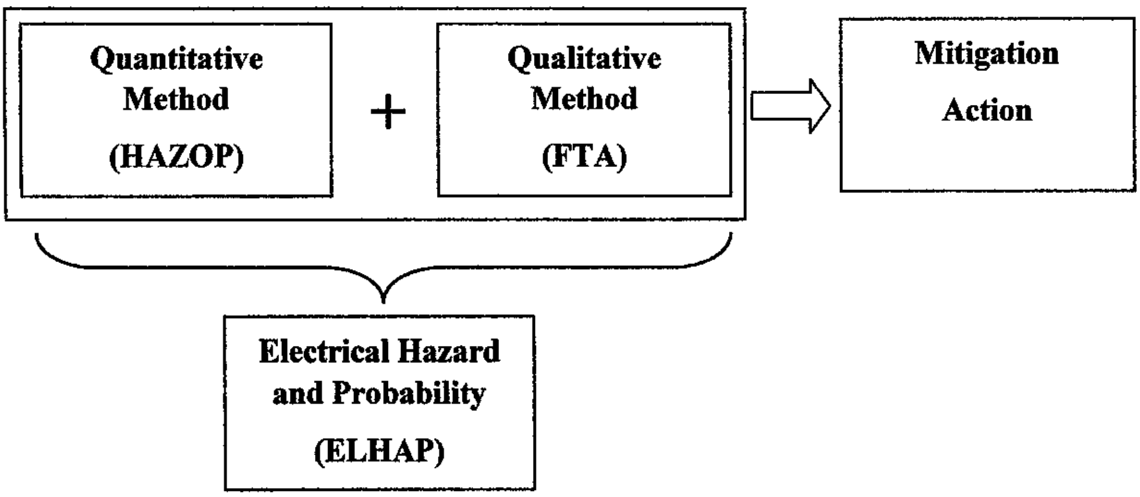


Figure 1: Basic concept of ELHAP

1.3 OBJECTIVES AND SCOPE OF STUDY

The main objectives of this research work are:

- To develop qualitative review or assessment of the problems due to electrical equipment and system failure in the plant by using HAZOP methodology approach
- To develop quantitative analysis tool based on FTA to rank the hazardous events
- To test the framework and tool developed using industrial case study

The scope of work for this project is mainly to provide a new framework for systematic identification and analysis of electrical hazards in the process plant due to electrical equipments and system failure. The framework or tool developed will be directly implemented in the industrial application to test for its efficiency and suitability. The project is considered significantly valuable due to the following reasons:

i. There is very limited detailed research that has been done on the same subject (electrical safety) so far. HAZOP approach is considered as one of the most complete guide for safety analysis but it mainly covers process units in general rather than auxiliary plant such as power generators.
ii. Combination of HAZOP and FTA approaches will provide a more detailed safety analysis. Many researchers only focus their researches on how to automate usage of HAZOP and FTA tools separately instead of combining them in a new single tool.
iii. The tool developed will help to provide stringent decision on actions that involve high cost or major changes to the design due to safety issues since it not only analyzes the potential hazards, but it gives probability for hazards with higher level of risk.

CHAPTER 2
LITERATURE REVIEW

2.1 SAFETY ANALYSIS

Process hazard analysis (PHA) ensures equipment safety and identifies the possible hazards that may arise as a result of equipment malfunctions and deviations of process variables (temperature, pressure, etc) from normal operation, and it uses various different techniques such as fault tree analysis (FTA), event tree analysis (ETA), what-if analysis, and Hazard and Operability (HAZOP) analysis **[1]**.

A system can be considered safe if it is free from accidents and unacceptable loss. Hazard in the system is a state or condition of the system that can, in the presence of a stimulus from the environment, lead to an accident or loss. Environment here refers to location or surroundings where the system operates. M. Berry (1998) stated that in order to make sure that a system is safe, the most important key are the identification of hazards and an analysis of what to do about the hazards [2].

In some cases, the cause of a hazard can be identified, and then it can be controlled or eliminated. For some other cases, often it is impossible to predict in advance all possible causes of all possible hazards. Thus, it is important to gather as much information as possible about a particular system to hope that this information allows detection of the causes of all hazards before they lead to accidents **[2]**.

Currently a number of analysis techniques are used for safety analysis. The used analysis techniques can be grouped into quantitative techniques and qualitative techniques. Qualitative techniques compare and classify safety based on experience of the team that analyzes the hazard, while the quantitative techniques compare and classify safety based on calculation results using mathematical models.

According to Rouvroye et al.(2002), all techniques can be used to analyze the safety of industrial processes but the results will be different from each other due to different analysis techniques that start with different actions, end with different actions and follow different path in between start and finish. The authors suggested that the analysis technique that covers the most aspects relevant to the specific situation is used to produce the best result [3].

Thus it is very important to provide a detailed study specifically designed for electrical system to cover more aspects related to electrical safety.

2.2 ELECTRICAL HAZARD

Electricity has been long recognized as a serious workplace hazard, exposing employees to electrical shock, electrocution, burns, fires, and explosions [4]. Electrical injury is caused by current passing through the body. The damage and injury to the body are proportional to the amount of current through the body and the current density [5].

Successful accident prevention relies to a large extent on knowledge about the causes of accidents. The causes of electrical fatalities at work, according to Williamson et al.(1998) can be classified into four major factors which are:

i. *Environmental events:* events or conditions resulting from the location of the accident; these conditions could not have been changed at that point in time (e.g., low lighting, wet floor or cramped conditions).
ii. *Equipment events:* events resulting from breakage or malfunction of machinery or tools that occur at that point in time.
iii. *Medical events*: events resulting from the current state of physical well-being (e.g., heart attack or diabetic or epileptic episode).
iv. *Behavioral events*: events resulting directly from human involvement (e.g., leaning too far into the path of machinery, touching an electrically charged object, etc.). **[6]**

It is very important to identify and analyze the possible hazard in the process plant that can be caused by all of the above factors including the equipment events, in this case due to electrical equipment and system failure to make sure that the plant operation is as safe as reasonably practicable (ALARP).

2.3 EFFECTS OF ELECTRIC CURRENT

An electric shock can result in anything from slight tingling sensation to immediate cardiac arrest. The severity depends on the following factors:

i. The amount of current flowing through the body
ii. The current's path through the body
iii. The length of time the body remains in the circuit
iv. The current's frequency

Burns are the most common shock-related injury. An electrical shock can result in an electrical burn, arc burn, thermal contact burn, or a combination of burns. Electrical burns occur when electric current flowing through tissues or bone, generating heat that cause tissue damage. Arc or flash burn results from high temperature caused by an electric arc or explosion near the body. Thermal contact burns occur when the skin touches hot surfaces of overheated electric conductors, conduits, or other energized equipments **[4]**.

Appendix A provides more details of general relationship between the amount of current received and the reaction to the body when current flows from the hand to foot in the basis of 1 second reaction time.

2.4 QUALITATIVE METHOD

Qualitative method is a type of hazard analysis that implements the experience and expertise in particular subject to analyze the hazards. There are a number of approaches that can be used to qualitatively analyze the hazard and one of them is to use hazard and operability method.

Hazard and operability study is a methodology for identifying and dealing with potential problems in industrial processes, particularly those which would create a hazardous situation or a severe impairment of the process. It is commonly known as HAZOP. It is said to be the most widely used method of hazard analysis in the process industries, notably the chemical, petrochemical and nuclear industries.

2.4.1 HAZOP analysis

In this project, HAZOP will be used as a basic qualitative tool to identify the possible hazard by means of achieving specified design intentions of a particular plant. The design intentions here refer to the specific purposes of designing the plant. HAZOP involves a team of experts to do the analysis in which it allows the members to brainstorm their opinions using their experience from within their specific fields of expertise. This method applies to processes either existing or planned for which the design information is available. The HAZOP team will need to identify the possible significant deviations that can affect each of the intention by referring to the P&ID of the plant, as well as to determine the related causes and consequences.

This procedure requires certain standard that need to be followed, which is to use a series of guidewords provided combining with the parameters that can cause deviations to each of the design intention. The combination of guidewords and the parameters will provide the cause of the possible deviations, and later they will be extended further to identify the consequences of the deviations. The deviations must have certain significance or consequences for them to be accepted as possible hazards. In this project, this is where quantitative FTA method will be integrated with HAZOP method to rank the possible hazards accordingly to make sure that high level risk is being prioritized. The current standard guide words used in HAZOP tools are as shown in **Table 1**.

Table 1: The standard current guide words used

(*Source: http://en.wikipedia.org/wiki/Hazop*)

Guide words	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN	Complete substitution
EARLY	Relative to the clock time
LATE	Relative to the clock time
BEFORE	Relating to order or sequence
AFTER	Relating to order or sequence

To make sure that specific focus is made to hazard related to electrical equipments and system failure, a series of physical parameters will be suggested. If the combinations between guide words and the physical parameters are meaningful or have certain significance, they are considered as potential deviations. Once the causes and consequences of each potential hazard have been determined and established, the system or operation being studied can be modified to improve its safety. In this project, certain recommendations will be provided along with specific causes of deviations to make sure that the plant safety can be optimized.

2.5 QUANTITATIVE METHOD

Quantitative method uses calculation results using mathematical models to assess the risk of identified possible hazards. This method is important to rank each of the possible hazards according to the level of risk it contains, and to what extent it is significant to be taken into consideration. The risk level here may depend on the likelihood of occurrence of the hazards, how often they occur (frequency), and how large are the impacts or consequences of the entire events (injuries or fatalities). Two most widely used methods in determining the risk level of the hazards are Fault Tree Analysis (FTA) and Event Tree Analysis (ETA).

2.5.1 Fault tree analysis method

Fault Tree Analysis or FTA method is used widely as a tool for quantitative risk assessments. It attempts to model and analyze failure processes of engineering systems. FTA is composed of logic diagrams that display the state of the system and is constructed using graphical design techniques to analyze top-level event that leads to possible hazards in term of sub-events, followed by lower order events, which eventually leads to individual events that have caused the top-level event. The basic elements of a fault tree may be classed as (1) the top event, (2) primary (basic) events, (3) intermediate events and (4) logic gates. The top event is normally some undesired event. Typical top events are flammable or toxic releases, fires, explosion and failures of various kinds. Primary (basic) events are events that require no further development. Intermediate events are the events in the tree between the top event and the primary events at the bottom of the tree. Logic gates define the logic relating the inputs to the outputs. The two principal gates are the AND gate and the OR gate. The output of an AND gate exists only if all the input exist. The output of an OR gate exists provided at least one of the input exists [7].

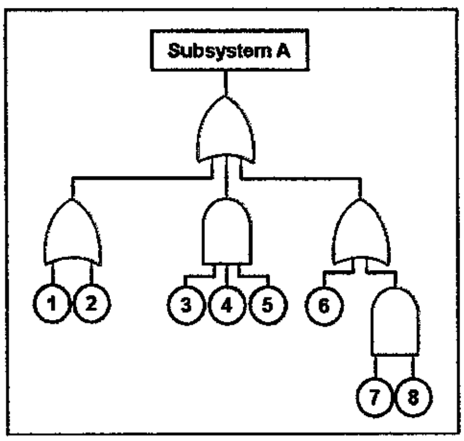


Figure 2: A Fault Tree Analysis diagram

(Source: http://en.wikipedia.org/wiki/Image:Fault_tree.png)

2.5.2 Basic Fault Tree Symbols

Figure 3 shows the basic symbols of the events used in FTA method, while **Figure 4** show the basic gate symbols used in the method.

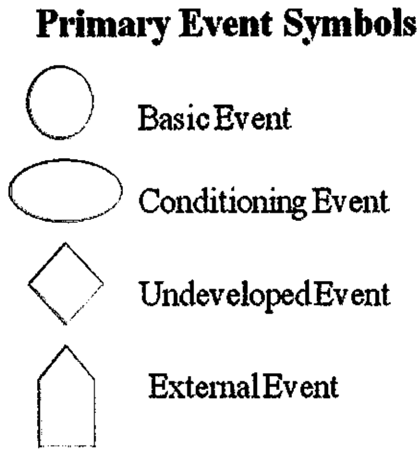


Figure 3: Primary event symbols used in FTA
(Source: http://en.wikipedia.org/)

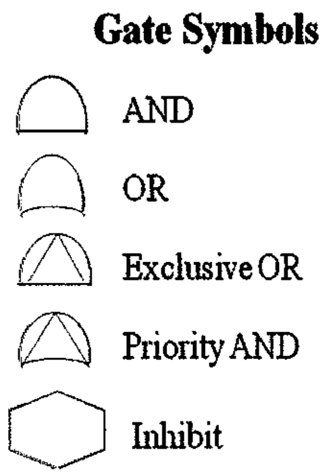


Figure 4: Gate symbols used in FTA
(Source://http://en.wikipedia.org/)

2.5.3 Limitation of FTA

Although obtaining the exact top event probability of the FTA is one of the most important aims in any analysis, it is a difficult problem for a reasonably large scale system with complex structure such as a chemical plant. According to S. Yanagi et al.(2008), the complex representation of FTA diagram for such plant are caused by several type of dynamic behaviors that exist in the analysis such as sequence dependency [8]. The limitation of reliability of FTA method in modeling the dynamic systems has also been discussed by Bucci et al. (2008) [9].

Markov modeling is an advance technique that can be used for dynamic system and time dependant failures but many engineers do not feel comfortable with Markov modeling and its fundamental mathematical background [10]. This project however does not consider dynamic properties of the system which will end up making the analysis more complex than it should be. In addition, electrical equipment and system failures usually do not significantly involves dynamic behaviors.

FTA can be used because it explicitly expresses how equipment failures and system failures can lead to potential hazards in a graphical representation that is easy to understand. It identifies major risk contributors and combinations of primary failures (and human errors) that lead to an undesirable incident. In particular, it quantifies benefits associated with process safe guards and compares risk-reduction measures quantitatively in terms of safety. It is a structured methodology and well documented, ready to modify according to system changes [10].

2.5.4 Failure rate

In order to calculate the probability or failure distribution of top events, probabilities or failure distributions of all basic events are required. Dearth of failure rate data and the large uncertainty associated with the data is a considerable problem in the application of FTA. With data collection and exchange efforts from both the government agencies and industry, this problem is slowly being ameliorated [10].

Failure rates depend on various factors including the function of the equipment, the definition of failures, the process conditions, and the maintenance plan. The ideal situation for a reliability study is to have sufficient plant data from identical equipment from the same process. However, in many cases, in-house data are not always available. For new plants, there are essentially no historical failure rate data. In those cases, generic data from external sources must be used [10].

There are various sources for failure rate database such as The Data Acquisition Working Party of the Mechanical Reliability Committee of the Institution of

Mechanical Engineers in the United Kingdom, Guidelines for Process Equipment Reliability Data with Data Tables by American Institute of Chemical Engineers, and Offshore Reliability Data Bank (OREDA) (1984, 1988, 1997, and 2002) **[10] [11] [12]**. A comprehensive compilation of failure rate and event data can also be found in *Loss Prevention in the Process Industries Volume 3* (Lees, 1996) **[13]**.

FTA in this project will use available Failure Rate Data of components and processes in the basic events from the above mentioned sources to estimate the probability of the top event.

2.5.5 Failure probability

The Failure Rate Data shows the average component failure over a period of time. This is called the failure rate and it is represented by μ with units of faults/time. The units used are usually failures per 10^6 hours. The probability the component will not fail during the time interval (0, t) is given by a Poisson distribution **[14]**.

$$R(t) = e^{-\mu t} \tag{2.1}$$

R = Reliability

μ = Failure rate (assumed constant), as $t \rightarrow \infty$ the reliability goes to 0

The complement of the reliability is called the failure probability, P and is given by

$$P(t) = 1 - e^{-\mu t} \tag{2.2}$$

P = Probability

μ = Failure rate (assumed constant), as $t \rightarrow \infty$ the reliability goes to 1

The failure probability is the value that is used in the probability calculation for every event. The sources of failure rate data available depend on user. It may be obtained from external sources such as the literature and data banks. Alternatively they may be collected within the works.

2.6 CURRENT TOOLS AVAILABLE

There are established indices such as the Dow Fire and Explosion Index (F&EI), the Mond Index, and the Instantaneous Fractional Annual Loss (IFAL) Index which can be used for systematically identifying hazards and providing a method of ranking priorities.

The Dow F&EI is the most widely used hazard index. It was originally developed by the Dow Chemical Company in 1964 to assist in the selection of fire protection methods. The analysis divides a plant into separate process units and assigns indices based on material properties, process conditions, areas of exposure, and other damage factors to derive the base maximum probable property damage (MPPD). Loss control credits are then applied to adjust MPPD to calculate actual MPPD. The guide has been updated several times but still only covers process units rather than auxiliary plant such as power generators **[10]**.

The Mond Index was developed by Imperial Chemical Industry (ICI) for the chemical industry, after the Flixborough disaster. The hazard is assessed in a similar way to the Dow F&EI index but introduces additional considerations. Initial assessments of fire, explosion and toxicity are carried out for each process unit. Offsetting factors for prevention and protection measures are then assigned and combined with initial indices. Finally, an overall risk rating is derived from individual fire, explosion, and toxicity indices. It provides a more comprehensive treatment of hazards from materials, reactions and toxicity **[10]**.

The IFAL index was originally developed for insurance assessment purpose by the Insurance Technical Bureau. It requires dividing the plant into blocks, and the contribution of each major item of process equipment is determined according to process factors, engineering factors, and management factors. Frequency and size of potential emissions and chance of ignition are used to determine damage **[10]**.

CHAPTER 3
METHODOLOGY

3.1 ELHAP PROCEDURES

Electrical Hazard and Probability (ELHAP) assessment consists of two main parts which are:

i. ***Hazard Identification (Qualitative Method):*** using similar approach to Hazard and Operability (HAZOP) analysis which uses guidewords in performing the analysis.

ii. ***Hazard Ranking (Quantitative Method):*** using Fault Tree Analysis (FTA) probability calculation method to rank the hazard according to the level of risk it possesses.

In order to integrate the two methods together, HAZOP and FTA approach must be synchronized, thus hazards are identified by using keywords and guidewords starting from the top event, similar to FTA analysis. In standard HAZOP method, guidewords is used to initiate causes of sub events from the deviation of parameters that will lead to the top event, but in the ELHAP, the top event is identified as the starting point. This to make sure that it is easier to calculate the probability of each identified hazard during the hazard ranking procedure later.

Special keywords and guidewords are introduced since original HAZOP guidewords are not suitable to be used to identify hazards starting from the top event. In the analysis, only top event that contributes to acceptable amount of risk is being ranked accordingly. This is to make sure that the assessment is as practical as possible. Details of the methodology are discussed further in the following sections.

3.2 TOOLS

3.2.1 Software Package

Usage of the following software is required if ELHAP is going to be implemented in an automated application form in the future:

i. Microsoft Excel: Software to develop table for the basic HAZOP analysis, and to rank the hazardous event accordingly using FTA tool.
ii. Visual Basic Application: Software that will be used to link the Microsoft Excel to the specific P&ID or SLD of the plant.

3.3 IMPLEMENTATION

It is important that the tool developed, ELHAP can be implemented in the real industrial cases. Safety consideration is very important in both design stage and also for on-going operation, thus the tool developed is aimed to be used for both situations. For this purpose, the following materials are required:

1. Process description
2. Process flow sheet in the form of Single Line Diagram (SLD)
3. Equipment and instrument specifications
4. Layout drawing
5. Operating procedures
6. Maintenance procedures

Figure 5 shows the suggested implementation inputs and outputs of the ELHAP. At the end of the study, ELHAP will provide suggestion to improve the system design, operation and maintenance procedures to optimize the safety and operability in the overall plant.

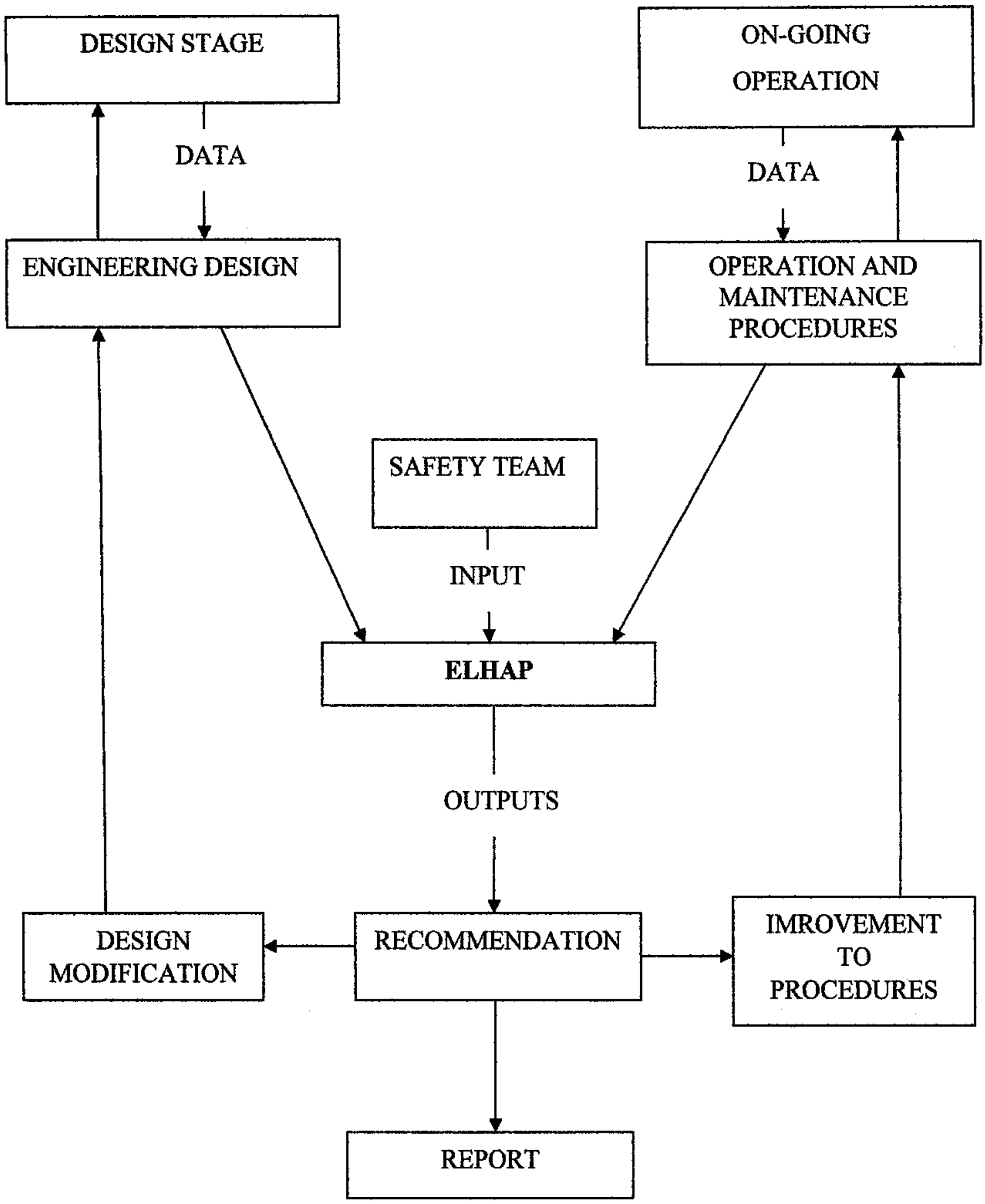


Figure 5: Implementation of ELHAP in system design, operation and maintenance procedures for new system design and on-going plant operation.

3.4 SAFETY TEAM

For an effective analysis, ELHAP requires involvement of group of experts in safety and electrical system since it is a team approach tool similar to HAZOP analysis. The following members are the suggested persons to form a team for the analysis:

i. Team leader
ii. Safety Officer
iii. Process plant operators
iv. Electrical maintenance engineer
v. Electrical design engineer
vi. Electrical technical manager
vii. Others as required

3.5 PROCEDURES

Based on the HAZOP approach which introduces parameters and guidewords and also the FTA concept, the following method is the suggested framework for ELHAP study:

i. Specific component of interest is specified in the process and instrumentation diagram (P&ID) of the process plant. The single line diagram (SLD) is usually used to focus on specific design intent of the electrical operation.

ii. Possible hazards are indentified to determine the type of possible hazards related to the specified component in general. The following are the possible **hazard keywords** suggested for each of the component:
   - Electrical shock
   - Fire
   - Explosion
   - Physical Threat
   - Toxicity
   - System Failure

iii. **Exposure situation** is determined according to the specified hazard keyword to identify the general condition/situation of the hazards. For each type of hazard, the following exposure situation is suggested:

- Electrical shock – direct contact, indirect contact
- Fire – normal, chain reaction, lightning
- Explosion – chemical, mechanical, electrical
- Physical Threat – individual, surroundings
- Toxicity – chemical, biological, physical
- System Failure – no power, low power, malfunction

iv. **Exposure elements** in the form of guidewords are applied in this stage to analyze the causes of the problems. Guidewords suggested consists of the following keywords related to the operation of the electrical equipments:

- IDENTIFY
- OPERATE
- CONTROL
- DISPLAY
- MAINTAIN
- FUNCTION

v. **Deviation** from normal operation is determined according to the selected guidewords. For each of the operation parameter, the following deviation is suggested:

- IDENTIFY – Fail to identify, false identification
- OPERATE – Fail to operate, fail to open, fail to close, fail to isolate
- CONTROL – Fail to control, false control
- DISPLAY – Fail to display, false display
- MAINTAIN – Fail to maintain
- FUNCTION – Fail to function

vi. Detailed causes of the hazards are determined according to the specified deviation.

vii. Consequences of the hazards are determined.

viii. If the consequences are significant, FTA probability calculation method is used to rank the hazards to make sure the highest risk hazard can be prioritized followed by the second highest, etc.

ix. Suitable recommendations will be suggested for further actions.

The procedure suggested above is simplified in the flow chart as shown in **Figure 6.** The detail definition for each of the terms (hazard keywords, exposure situation, guide words, etc) used in the procedure above can be found in the **Appendix B.**

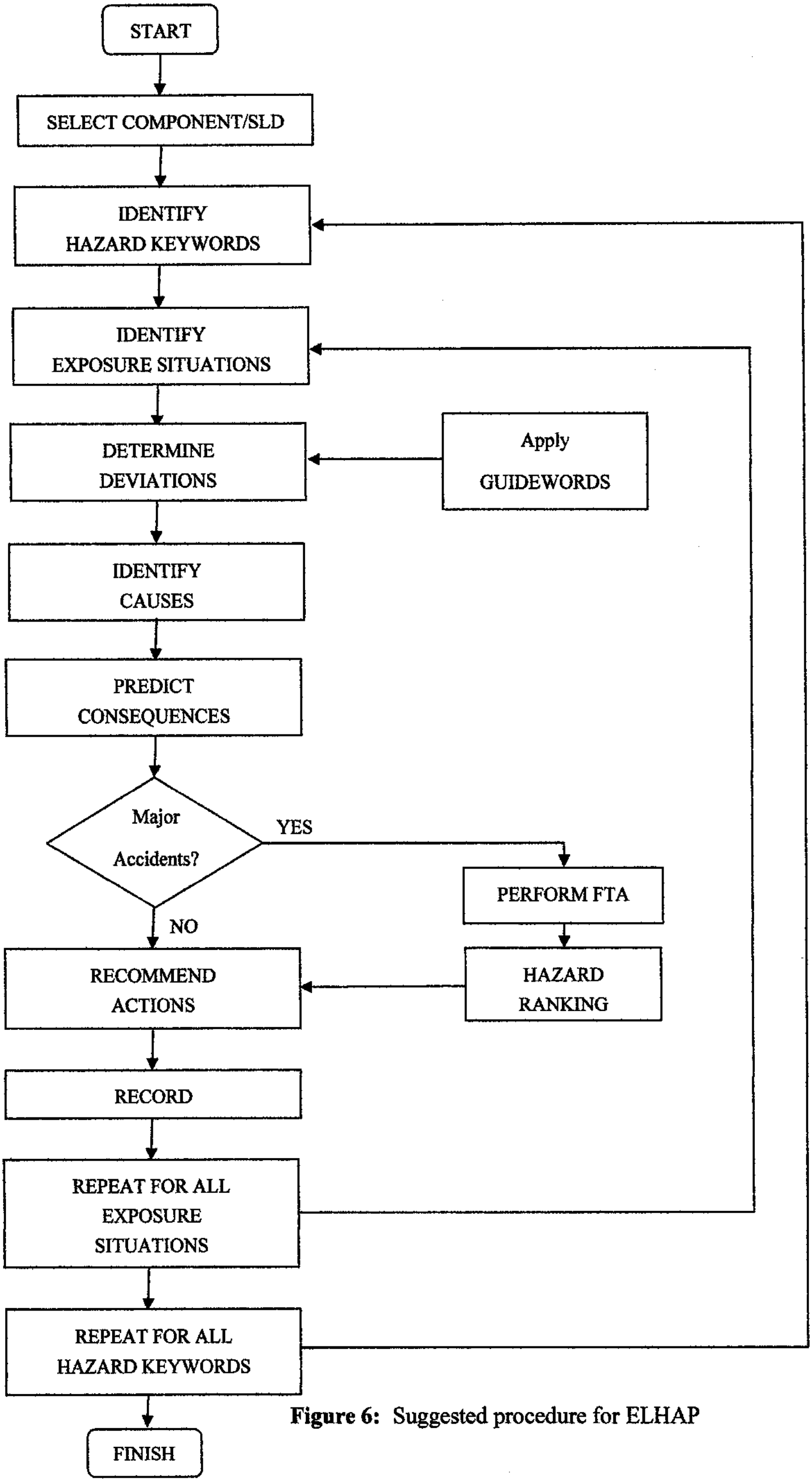


Figure 6: Suggested procedure for ELHAP

The information gathered during the procedure above can be recorded in a table as suggested in **Table 2.** The Fault Tree Analysis will be performed only if the consequences are very significant in which it gives major impact to the system design or plant operation. It will be discussed further in the following **Section 3.6.**

Table 2: Suggested table for ELHAP study

Item	Hazard Keyword	Exposure Situation	Exposure Elements (GUIDEWORDS)	Deviation	Causes	Consequences	Probability (*FTA result)	Recommendation	Action
	Electrical Shock	Direct contact Indirect contact	IDENTIFY	Fail to identify False identification					
	Fire	Normal Chain reaction Lightning	OPERATE	Fail to operate Fail to open Fail to close Fail to isolate					
	Explosion	Chemical Mechanical Electrical	CONTROL	Fail to control False control					
	Physical Threat	Individual Surroundings	DISPLAY	Fail to display False display					
	Toxicity	Chemical Biological Physical	MAINTAIN	Fail to maintain					

	System Failure	No power Low power Malfunction	FUNCTION Fail to function					

*FTA result is in the form of probability of occurrences of each of the hazardous event ranging from 0 to 1.0. As the probability increases, the level of risk the hazard possesses increases.

A simple example of the ELHAP analysis using the procedure as described in the **Section 3.5** is as shown in **Table 3** below. In this analysis, a component of the electrical system, in this case a gas turbine system is chosen as the subject.

Table 3: Example of analysis using suggested procedures

Component	Gas turbine system
Type of hazard	Electrical shock
Exposure situation	Direct Contact
Exposure element (Guideword)	OPERATE
Deviation	Fail to open
Cause	Switch fail to open
Consequences	Short circuit
Recommendation	Possibility to install additional over current protection
FTA result	0.0 – 1.0

3.6 FAULT TREE ANALYSIS (FTA) METHOD

3.6.1 FTA Procedures

In the ELHAP analysis, Fault Tree Analysis (FTA) method will be implemented to rank the hazardous events if the events possess significant consequences and they can be considered as major events. The significant consequences here may include:

i. Events which are considered very dangerous to the personnel operating the machines or equipments during the operation where they may cause major injuries or in the worst case scenario; fatality to the personnel.

ii. Events which contribute to considerable amount of loss to the plant operation, or to the company in general in term of money, or other resources.

Hazard ranking is required to rearrange all of the events with very significant consequences according to their probability and eventually to prioritize the event at which its consequences are more significant among all other events. The following are suggested procedures to rank the hazardous events accordingly based on FTA method:

iii. The top event or the hazardous event which is identified from the previous methodology is determined

iv. Possible faults or causes that must occur for the top event to occur are listed by branching down the top event to the smaller sub-events.

v. During this branching procedure, sequential, parallel or combinations of sub-events are considered to make the analysis as accurate as possible. This can be done by using standard fault tree symbols. In this project, only "AND" and "OR" gates are used since they are widely used to represent the causes for each of the event.

vi. Boolean algebra is used to quantify fault tree with event probabilities in order to determine the top event probability.

vii. Event with highest probability ranks first, and it must be prioritized when actions are being taken to mitigate the hazard.

3.6.2 Probability Calculation

Before proceeding with the top event probability, the probability value of each of the basic event is calculated by using the following equation:

$$P(t) = 1 - e^{-\mu t} \tag{3.1}$$

P = Probability

μ = Failure rate (assumed constant), as $t \rightarrow \infty$ the reliability goes to 1 (faults/10^6 h)

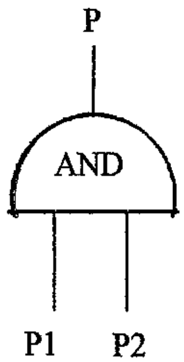
t = time (10^6 h)

[14]

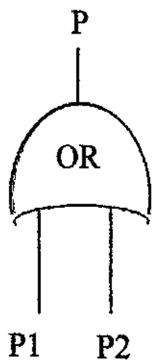
As discussed before in the **Section 2.5.4**, the failure rate data can be determined either from manufacturer or from failure rata data handbooks. Failure rate data collected from various established sources for some selected electrical equipments together with their respective values of probability can be found in **Appendix D.**

3.6.3 Boolean algebra

Once the Fault Tree diagram has been developed, Boolean equations can be derived to evaluate the probability estimates for the sub-events. Combination of the sub-events probabilities will give the probability for top event. In this project, focuses will be made on "OR" and "AND" gates. The probabilities of the sub-events involving "OR" gates simply acts in additive manners while the probability of the sub-events involving AND gates will act in multiplicative manner. The basic formula for "OR" and "AND" gate cases are as follow:



$$\boxed{P = P1 \times P2} \tag{3.2}$$



$$\boxed{P = 1 - (1 - P1)(1 - P2)} \tag{3.3}$$

For more complex tree diagram, in the case an event is connected to its causal events by an AND gate, the probability of its occurrence is given by the relationship:

$$P = \prod_{i=1}^{n} P(E_i) \tag{3.4}$$

For a case where all the events are connected to an event via an OR gate, the probability of the event is given by the relationship:

$$P = \prod_{i=1}^{n} [1 - P(E_i)] \tag{3.5}$$

Where

P = the probability of occurrence of the event immediately above the AND or OR gate

P (E_i) = probability of occurrence of events immediately below the AND or OR gate

n = the number of events immediately below the OR gate

$\prod$ = the symbol for multiplication

[15]

The complete guide for Boolean algebra for Fault Tree Analysis can be referred to in **Appendix C.** In this guide, formulas to determine probability involving combinations of both "AND" and "OR" gates in various situations are shown.

CHAPTER 4
RESULT AND DISCUSSION

4.1 INDUSTRIAL CASE STUDY

Implementation in industrial case study is very important to make sure that the framework developed is not just theoretically sound but it is also practical for real life applications. The location for the main industrial case study has been chosen to be at the Lumut Power Plant (LPP) in Lumut, Perak. The reason for selection of Lumut Power Plant as the location for industrial case study is because:

i. Lumut Power Plant is located nearby, thus it is easier for the research to be done at anytime during the commencement of the semester.
ii. The focus of this study is specifically more onto electrical system, thus it is great if it is done directly at the electrical power system before doing direct implementation at electrical system in process plant.

Based on the procedures discussed in **Chapter 3**, an industrial case study will be implemented at Lumut Power Plant. For this purpose, the single line diagrams for the whole plant and gas turbine have been obtained from the power plant. Please refer to **Appendix E** for the single line diagram of the whole plant.

Additional case study was done for the 110V Alternate Current Uninterruptible Power Supply (AC UPS) at PETRONAS Fertilizer Kedah Sendirian Berhad (PFKSB) to further test the suitability of the ELHAP assessment. Please refer to **Appendix G** for the single line diagrams of the AC UPS system.

4.2 LPP HIGH VOLTAGE GAS TURBINE SYNCHRONIZATION STEPS

4.2.1 Gas turbine system

Gas turbine system is one part of the power plant system in Lumut Power Plant. Please refer to **Appendix F** for the gas turbine single line diagram. A gas turbine also known as combustion turbine is a rotary engine that extracts energy from a flow of combustion gas. It has an upstream compressor coupled to a downstream turbine, and a combustion chamber in-between.

According to Lumut Power Plant safety guidelines, high voltage apparatus include any equipment and conductors which are normally operated at a voltage of 15.75 kV and above. High voltage synchronization steps involve a series of high voltage switching. High voltage switching is defined as operation of high voltage switchgears, isolators or other methods of making or breaking a circuit. If a high voltage circuit can be energized or reenergized by means of low voltage equipment, such energizing or reenergizing shall be regarded as high voltage switching **[16]**.

4.2.2 Safety clearances from live conductors

When work is to be carried out in the vicinity of any exposed high voltage conductor which is or can be made live, the section which is made dead for work to be carried out shall be defined as far as possible by the use of approved barriers or approved roping arrangements. The minimum clearance from such exposed conductor to ground level or platform or access way shall be as given in the **Table 4** below:

Table 4: Minimum clearance from exposed conductor for different voltage

Rated Voltage	**Clearance**	
	Metric	Imperial
2.1 kV & 6.6 kV	2590mm	8' 6"
15.75 kV	2740mm	9' 0"
275 kV	4570mm	15' 0"

4.2.3 Isolation step

The following are the isolation steps that need to be obeyed before the synchronization steps or other testing take place:

a) Equipment shall be made dead by opening the appropriate circuit breakers and Isolators links.

b) Isolation shall be obtained by opening Isolators or links, or racking out circuit breakers or removing fuses. Where appropriate, air isolation together with positive action to ensure that the closing mechanism is inoperative, will be acceptable instead.

c) Neutral point connections which may be subject to a rise of potential shall be as in paragraph (a) above if deemed required by the electrical competent person

d) Possible back feeds from the Low Voltage sides of power transformers, voltage transformers or auxiliary transformers shall be removed by isolating the Low' Voltage sides of the transformers, as in paragraph (a) and/or (b) above.

4.2.4 Synchronization steps

Based on the guidelines given, the high voltage gas turbine synchronization steps involve pre-condition step and high voltage switching step as follow:

4.2.4.1 Pre Condition

i. Equipment in open status – S38,S30,S34,W36,W30,W34,S48,S40,S44

ii. M3 De-energized

iii. R3 Energized GT31,GT32,GT33,Ayer Tawar 4

iv. GT31 back feed via R3-M96-M90-M93

4.2.4.2 Switching Steps

i. GT31 is running and already synchronized through R3 at operating watt via circuit breaker.
ii. Open M90 by DCS command and GT31 stay idle
iii. Open M90 > Open M96 > Close M94
iv. Black sync M90 via M94 to dead M3 bus > Completed
v. Open M90 by power plant > Close W36 > Close W34 > Close W30 energized M3 with TNB power
vi. HV sync M90 through M94 to M3
vii. Complete HV CB sync

4.2.5 ELHAP Analysis

Based on the procedures developed in **Section 3.5**, the following table, **Table 5** can be constructed for the gas turbine system. This table has been developed according to the suggested hazard keywords, exposure situations, guidewords, and associated deviations as shown in **Table 2.** Three major hazards are identified in this case study. The FTA results in the **Table 5** are obtained using previously explained method in **Section 3.6**. The details of the FTA analysis for both hazards are as shown in **Figure 7** and **Figure 8**, respectively.

Table 5: ELHAP analysis for gas turbine synchronization system

Type of hazard	Exposure situation	Exposure element (GUIDEWORDS)	Deviation	Causes	Consequences	*FTA	Recommendation
Electrical shock	Direct contact	OPERATE	Fail to open	Fail to open S38, S30, and S34 Fail to open S48, S40, and S44 Fail to open W30, W34, and W36	System is not isolated properly – may cause injury to personnel ranging from burn to death	0.02722	Make sure every isolation steps are followed properly Check for any failure of the switches before proceeding with the next procedures
			Fail to isolate	Fail to isolate ST34, GT32, or GT31.	May cause injury to personnel ranging from burn to death		
Explosion	Electrical	OPERATE	Fail to open Fail to close Fail to isolate	Fail to open M90, M96 Fail to close M94 Fail to isolate M3 bus	Electrical current fault flow – very high voltage flow may cause sudden explosion damaging the circuit	0.8380	Make sure every isolation steps are followed properly Check the controller before proceeding
		FUNCTION	Fait to function	Circuit breaker at GT31, fail to function	Over voltage flow may cause electrical explosion.		Make sure circuit breaker at GT31 is working properly
		DISPLAY	False display	DCS display that the M90 as open (should be closed)	Over voltage flow may cause electrical explosion.		DCS command system must be checked to make sure it works properly

System Failure	No power	MAINTAIN	Fail to maintain	Fail to maintain all required power supply from TNB power generation station	Gas turbine synchronization steps cannot be completed		Make sure to maintain adequate power supply from TNB power generation station
	Low power	MAINTAIN	Fail to maintain	Fail to maintain adequate power supply from TNB power generation station	Gas turbine synchronization steps cannot be completed		Make sure to maintain adequate power supply from TNB power generation station

4.2.6 FTA Method

The fault tree analysis diagram can be developed to track all of the sub-events or faults that may contribute to occurrences of the major hazard identified in the gas turbine system. The failure rate data of the basic events and its associated probability of failure are taken from **Appendix D.** The Fault Tree Analysis is conducted only for event that produces acceptable amount of risks or consequences, in this case, the electrical shock and explosion. Fault Tree Analysis diagrams for electrical shock and explosion hazard in gas turbine are as shown in **Figure 7** and **Figure 8**, respectively.

Figure 7 show that the probability of electrical shock in the gas turbine system is calculated to be 0.02722; while **Figure 8** shows that the probability of the explosion in the gas turbine system is 0.8380. It shows that the probability of explosion in the gas turbine system is very high, and the recommended action must be taken into consideration more seriously before starting any operation related to the gas turbine system.

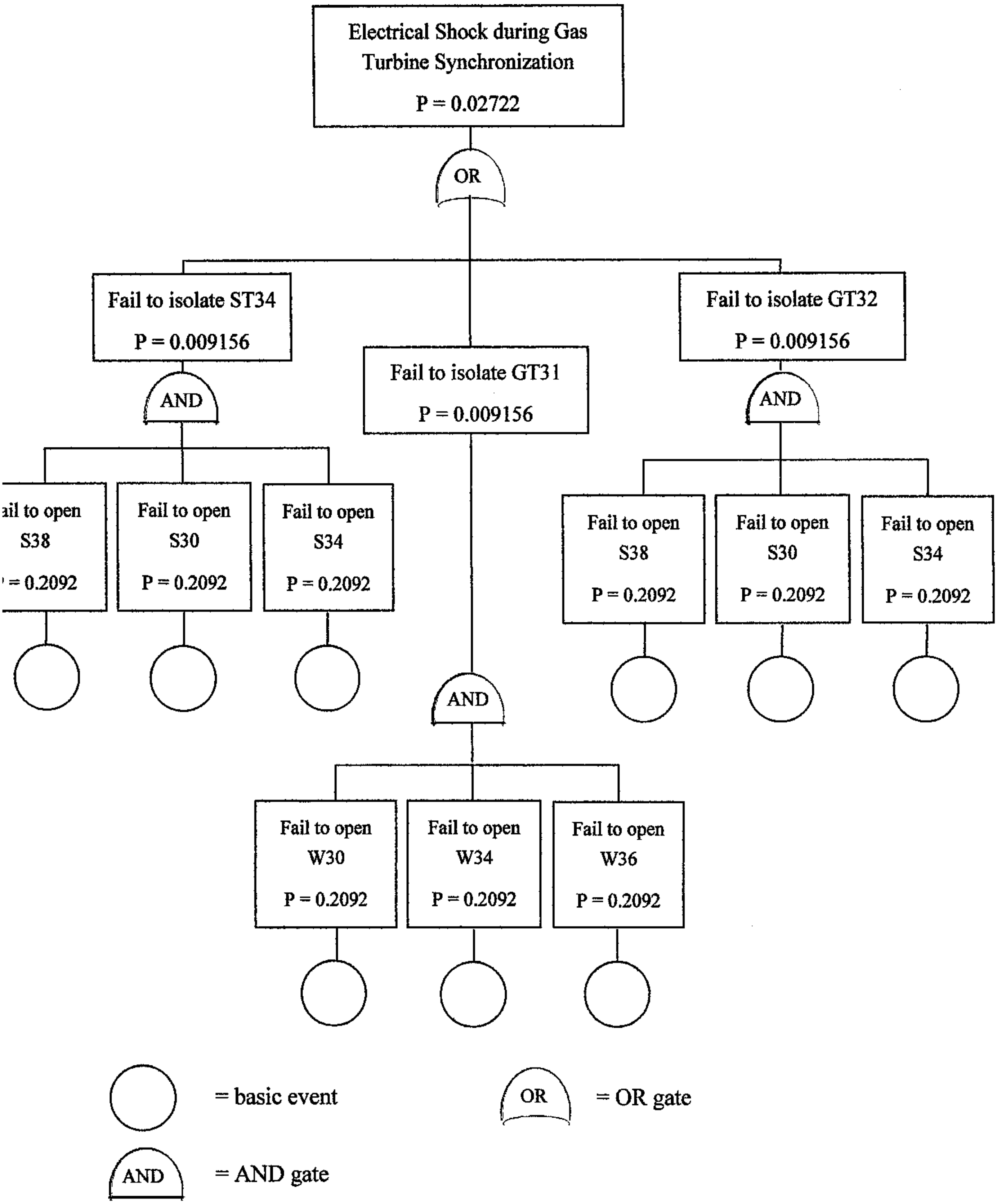


Figure 7: FTA analysis for the electrical shock hazard in the gas turbine system

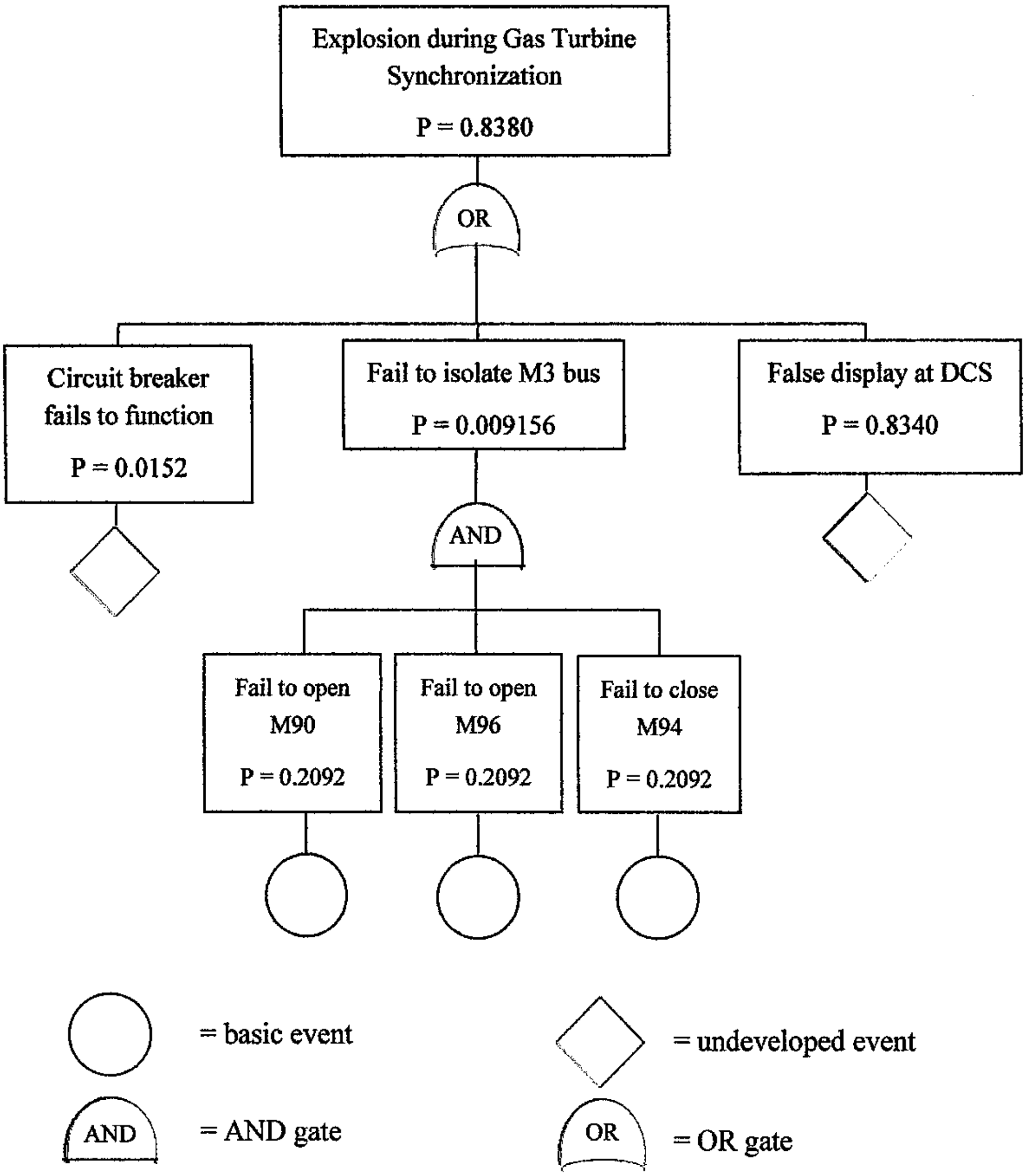


Figure 8: FTA analysis for the explosion hazard in the gas turbine system

4.3 PFKSB 110V ALTERNATING CURRENT UNINTERRUPTIBLE POWER SUPPLY (AC UPS)

110V AC UPS units comprises of rectifier, inverter, by-pass system and stand-by battery for the installation. The following **Figure 9** shows typical arrangement layout- Parallel Operation extract of AC UPS from PETRONAS Technical Standard (PTS). Detail drawing is as shown in **Appendix G.** General design consideration and operating conditions for the AC UPS system are shown in **Appendix H.**

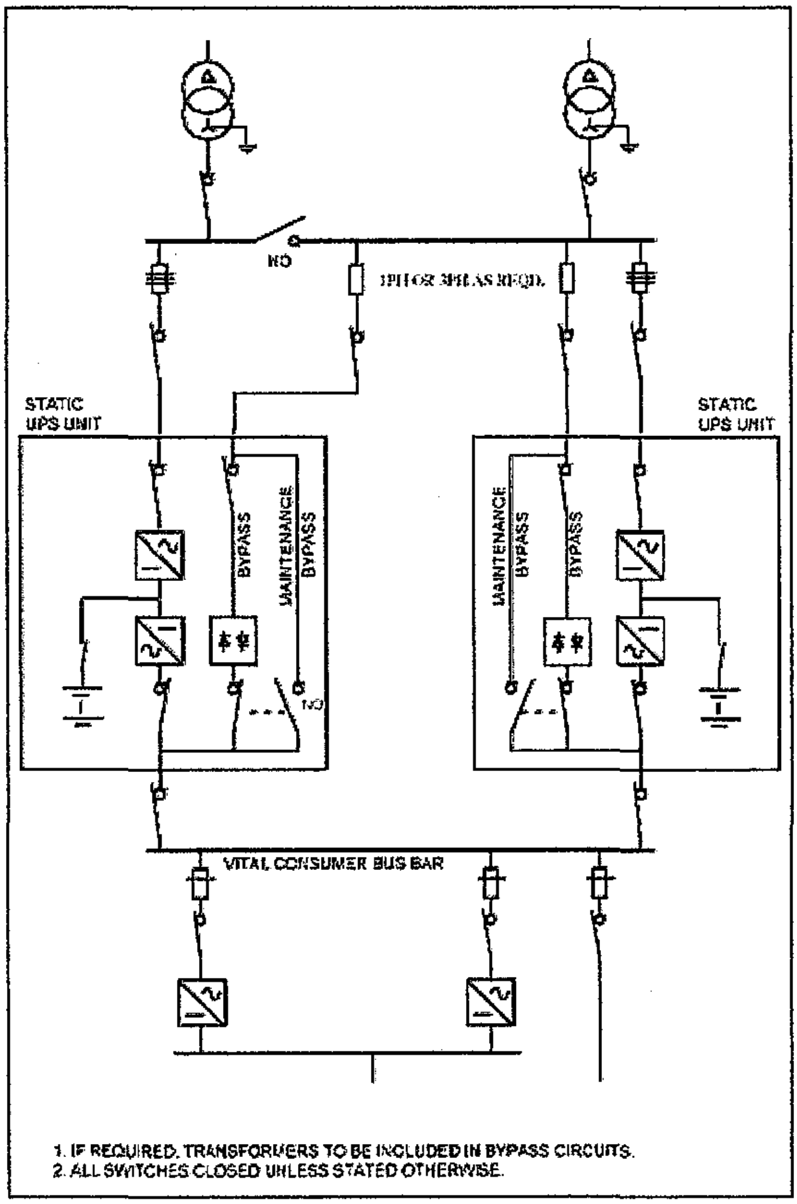


Figure 9: Typical arrangement of AC UPS system

4.3.1 ELHAP Analysis

The following **Table 6** shows ELHAP Assessment for the Alternating Current Uninterruptible Power Supply (AC UPS) at PFKSB. The major hazard identified during the operation of the AC UPS is electrical shock during maintenance procedures and system failure during the operation.

4.3.2 FTA Analysis

For this case study, both events contributes to considerable amount of risk since electrical shock may cause injury (or death) to personnel, while system failure may cause shutting down of operation, which will consequently affect the overall plant operation. This may cause considerable amount of losses to the company since the plant need to be operated continuously most of the time to cater for the product demand. The fault tree (FTA) analysis for the AC UPS system is as show in **Figure 10** and **Figure 11** respectively. The failure rate data of the basic events and its associated probability of failure are taken from **Appendix D**. The FTA results show that the recommended steps that may reduce or eliminate the system failure event must be prioritized due to its higher probability of occurrences than the electrical shock hazard.

The higher the probability of occurrences for a particular top event or hazard in the system, the higher it ranks among the hazards identified. By doing the probability calculation, hazard with high likelihood to occur can be prioritized, followed by less risky hazards. If the system design or the operating and maintenance procedures are to be improved, more focus must be given to the improvement related to prevention of hazard with highest probability first.

Table 6: ELHAP analysis for the AC UPS system

Type of hazard	Exposure situation	Exposure element (GUIDEWORDS)	Deviation	Causes	Consequences	FTA	Recommendation
Electrical shock	Direct contact	OPERATE	Fail to open	Fail to open switch at maintenance by pass line Fail to open switch at static by-pass line	System is not isolated properly – may cause injury to personnel ranging from burn to death	0.08593	Make sure every isolation steps for maintenance procedures are followed properly Check for any failure of the switches before proceeding with the next procedures
			Fail to isolate	Fail to isolate Static UPS unit 1, and Static UPS unit 2	May cause injury to personnel ranging from burn to death		
System Failure	Malfunction	FUNCTION	Fail to function	Rectifier, inverter fail to function Fuse fail to function	System fail to operate properly may result in shutting down of operation	0.3002	Make sure to use equipments that follow the standards, check for equipment failure regularly.
	No/Low power	MAINTAIN	Fail to maintain	Fail to maintain adequate power supply from the AC input	System fail to operate properly may result in shutting down of operation		Make sure to maintain adequate power supply from AC input
		FUNCTION	Fail to operate	Backup Ni-Cd Battery fail to function/ disconnected			Make sure the battery fulfills standard requirement, check the battery regularly

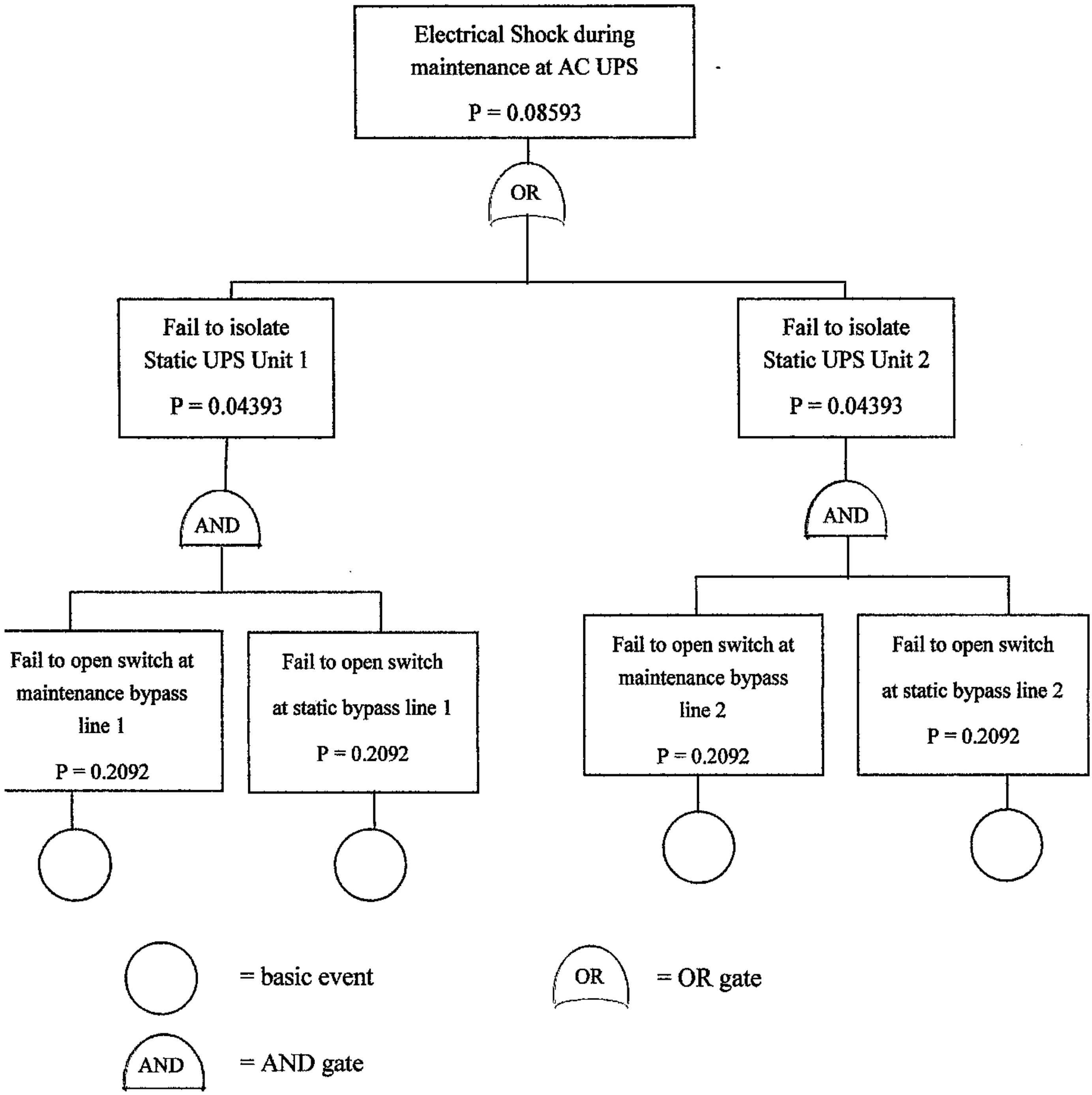


Figure 10: FTA analysis for the electrical shock hazard at AC UPS System

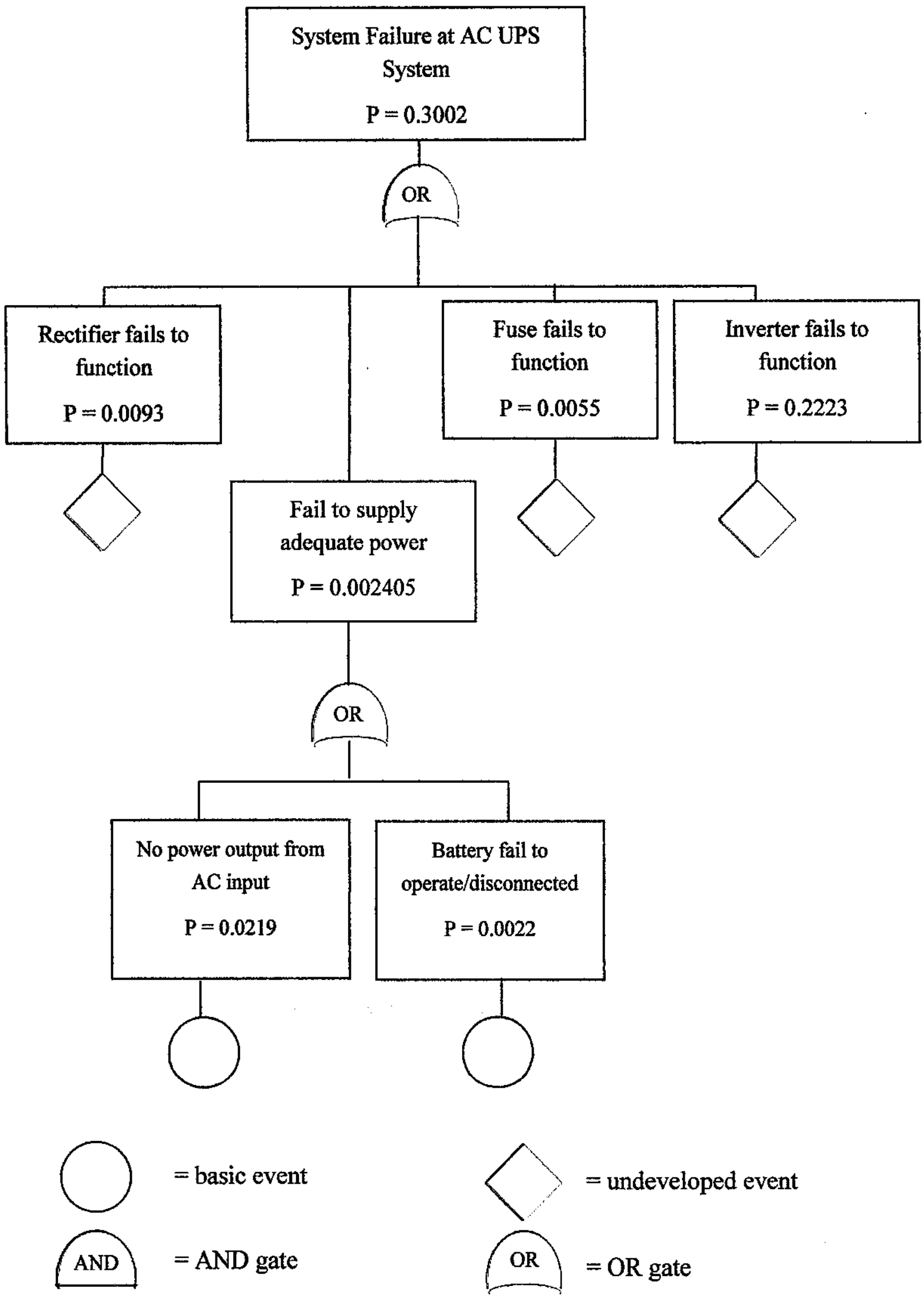


Figure 11: FTA analysis for the system failure at AC UPS system

4.4 COMPARISON WITH OTHER TOOLS

There are established indices which can be used for systematically identifying hazards and providing a method of ranking priorities in a chemical plant. Three most widely used indices are the Dow Fire and Explosion Index (F&EI), the Mond Index, and the Instantaneous Fractional Annual Loss (IFAL) Index **[10]**. The following **Table 7** shows the side by side comparison between ELHAP and the other three available methods.

Table 7: Side by side comparison between ELHAP and other methods

Specification	ELHAP	Dow F&EI	Mond Index	IFAL Index
Field of study	Electrical System in Chemical Plant	Developed by Dow Chemical Company in 1964 for Chemical process safety	Developed by Imperial Chemical Industry for Chemical process safety	Originally developed by Insurance Technical Bureau for insurance assessment purpose and its use is now extended to Chemical process safety
Specific safety coverage	Hazards in electrical system – equipment and system failures	Originally for fire protection. Revised several times to include explosion in chemical plant.	Fire, explosion and toxicity in chemical plant. Provides more focus on material, reaction and toxicity	Insurance assessment Hazards related to chemical process – ignition, emission in the process
Hazard Identification	HAZOP Approach with simple guidewords and safety terms.	Own approach. Defining material, and determine general and special process hazards.	Own approach. Basically use the same method as Dow F&EI with addition considerations	Own approach – dividing plants into blocks, and contribution of hazard for each block is based on various factors

Ranking Method	FTA approach to calculate the probability using available Failure Rate Data. This is a standard used everywhere.	Maximum Probable Property Damage (MPPD), calculated from Chemical Exposure Index (CEI) based on material factors, hazard factors, process factors. Own method of ranking.	Extended assessment of Dow F&EI – considering additional factors. Own method of ranking	Process factors, engineering factors and management factors to estimate damage. Own method of ranking
Complexity	Simple and easy to understand guidewords and safety terms	New safety terms (MPPD, and other related factors)	Safety terms based on Dow F&EI plus additional factors	New safety terms (process factors, engineering factors, management factors)
Transposable	Yes – can be easily extended for chemical process	No – only for fire and explosion. Calculation method for electrical is not considered.	No – only for fire, explosion and toxicity	Yes but must be modified to include other considerations which may cause it to be more complex.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 CONCLUSION

Combination of the concept of HAZOP and FTA methods to form a new framework for safety analysis, ELHAP is a very good initiative for a complete risk assessment especially in the area of electrical equipment and system failure which has not been discovered thoroughly. The HAZOP approach will help to identify all of the possible hazards in the electrical system, while the use of FTA method will help to prioritize the major hazards accordingly. At the end of the analysis, ELHAP will be able analyze and minimize the potential hazards due to electrical equipments and system failure to ultimately optimize the safety and operability in the plant by improving the system design, installation, operation and maintenance procedures.

5.2 RECOMMENDATION

The following are the recommendations in order to improve this project further:

i. It is very useful if a method to estimate the probabilities of occurrences for sub-events can be developed so that the probability for the top event can be easily calculated without relying so much on the data from others.

ii. It will be very useful if the identified major hazards can be ranked according to their severity in form of total cost of loss, number of fatality or injury and etc. in addition to ranking according to frequencies of likelihood to occur alone. This will provide more accurate probability distribution.

iii. If possible, the developed framework can be integrated into user-friendly software for an easy and automated access to all hazard information of particular component in the electrical system.

REFERENCES

1. Rahman S., Khan F., Veitch B., Amyotte P., 2009, "*$ExpHAZOP^+$: Knowledge-based expert system to conduct automated HAZOP analysis*", Journal of Loss Prevention in the Process Industries, doi: 10.1016/j.jlp.2009.01.008.

2. Berry D.M., 1998, "The Safety Requirements Engineering Dilemma", *IWSSD 1998: Proceedings of the 9th International Workshop on Software Specification and Design*, IEEE Computer Society.

3. Rouvroye J. L., van den Bliek E. G., 2002, "Comparing Safety Analysis Techniques", *Journal of Reliability Engineering and System Safety* **75 (3)**, p.289-294

4. Elanie L. C., Henshaw J. L., 2002, "*OSHA 3075*", Occupational Safety and Health Administration, U.S. Department of Labor.

5. Tooley M., 2004, "Electrical hazards: their causes and prevention", *Anaesthesia and Intensive Care Mediciene* **5 (11)**, p.366-368

6. Williamson A., Feyer A. M., 1998, "The Causes of Electrical Fatalities at Work", *Journal of Safety Research* **29 (3)**, p.187-196

7. Lees, Frank P.1996, *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, Vol.1, 2nd Edition, Butterworths, London

8. Yuge T., Yanagi S., 2008, "Quantitative analysis of a fault tree with priority AND gates", *Journal of Reliability Engineering and System Safety* **93 (11)**, p.1577-1583

9. Bucci P., Kirschenbaum J., Anthony M. L., Aldemir T., Smith C., Wood T, 2008, "Construction Of Event-Tree/Fault-Tree Models From A Markov Approach To Dynamic System Reliability", *Journal of Reliability Engineering and System Safety* **93 (11)**, p.1616-1627

10. Wang, Yanjun., 2004, *Development of a Computer-Aided Fault Tree Synthesis Methodology for Quantitative Risk Analysis in the Chemical Process Industry*, Texas A&M University .

11. American Institute of Chemical Engineers. 1989, *Guidelines for Process Equipment Reliability Data with Data Tables*, Center for Chemical Process Safety

12. Offshore Reliability Data : OREDA-84

13. Lees, Frank P.1986, *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, Vol.3, 2nd Edition, Butterworths, London

14. Crowl, Daniel A., and Louvar, Joseph F. 1990, *Chemical Process Safety: Fundamentals with Applications*, Prentice Hall

15. Mohd. Shariff A., Hussan N. A., Binay K. Dutta, 2008, *A Fault Tree Analysis Tool Developed in Microsoft Excel*, Universiti Teknologi PETRONAS.

16. Lumut Power Plant (LPP) Electrical Safety Procedure, 2003.

APPENDIX A

GENERAL RELATIONSHIP BETWEEN THE AMOUNT OF CURRENT RECEIVED AND THE REACTION

Current	**Reaction**
Below 1 milliampere	Generally not perceptible
1 milliampere	Faint tingle
5 milliamperes	Slight shock felt; not painful but disturbing. Average individual can let go. Strong involuntary reactions can lead to other injuries.
6–25 milliamperes (women)	Painful shock, loss of muscular control*
9–30 milliamperes (men)	The freezing current or "let-go" range.* Individual cannot let go, but can be thrown away from the circuit if extensor muscles are stimulated.
50–150 milliamperes	Extreme pain, respiratory arrest, severe muscular contractions. Death is possible.
1,000–4,300 milliamperes	Rhythmic pumping action of the heart ceases. Muscular contraction and nerve damage occur; death likely.
10,000 milliamperes	Cardiac arrest, severe burns; death probable

* If the extensor muscles are excited by the shock, the person may be thrown away from the power source.

Source: W.B. Kouwenhoven, "*Human Safety and Electric Shock*", Electrical Safety Practices, Monograph, 112, Instrument Society of America, p. 93. November 1968.

APPENDIX B

DEFINITION OF RELATED TERMS

1. General type of hazards (Hazard Keywords)

i. **Electrical shock** can occur upon contact of a human's body with any source of voltage high enough to cause sufficient current through the muscles or hair. The minimum current a human can feel is thought to be about 1 milliampere (mA).

ii. **Fire** is the heat and light energy released during a chemical reaction, in particular a combustion reaction.

iii. **Explosion** is a sudden increase in volume and release of energy in an extreme manner, usually with the generation of high temperatures and the release of gases.

iv. **Physical Threat** refers to any physical activities that can cause danger to the individuals.

v. **Toxicity** is the degree to which a substance is able to damage an exposed organism.

vi. **System Failure** refers to malfunction of part or the whole system of interest that contributes to sudden stop of the operation.

2. Exposure Situation (specific types of hazard)

Electrical Shock	Direct Contact	The personnel has direct contact with the exposed electrical parts
	Indirect Contact	The personnel has indirect contact with the electrical elements such as electromagnetic waves.
Fire	Normal	Normal fire caused by existence of adequate supply of oxygen, heat and fuel, without any further reaction that may contribute to chain reaction

	Chain Reaction	Normal fire that is associated with further reaction or continuous or growing supply of fuel, oxygen and heat to be able to sustain a chain reaction.
	Lightning	Fire that suddenly caused by lightning that may lead to normal or chain reaction fire.
Explosion	Chemical	The most common artificial explosives are chemical explosives, usually involving a rapid and violent oxidation reaction that produces large amounts of hot gas.
	Mechanical	Strictly a physical process, as opposed to chemical or nuclear, eg, a the bursting of a sealed or partially-sealed container under internal pressure is often referred to as a 'mechanical explosion'. Examples include an overheated boiler or a simple tin can of beans tossed into a fire.
	Electrical	A high current electrical fault can create an electrical explosion by forming a high energy electrical arc which rapidly vaporizes metal and insulation material. Also, excessive magnetic pressure within an ultra-strong electromagnet can cause a magnetic explosion.
Physical Threat	Individual	Physical hazard cause by individual carelessness or medical problems that lead to instabilities in orientation, abnormalities in work, etc.
	Surroundings	Physical hazard cause by the environment where the personnel works due to surrounding problems such as instabilities of structures, etc.

Toxicity	Chemical	Chemicals include inorganic substances such as lead, hydrofluoric acid, and chlorine gas, organic compounds such as methyl alcohol, most medications, and poisons from living things.
	Biological	Biological toxic entities include those bacteria and viruses that are able to induce disease in living organisms.
	Physical	Physically toxic entities include things not usually thought of under the heading of "toxic" by many people: direct blows, concussion, sound and vibration, heat and cold, non-ionizing electromagnetic radiation such as infrared and visible light, and ionizing radiation such as X-rays and alpha, beta, and gamma radiation.
System Failure	Malfunction	Part of the system or the whole system fails to function normally according to design intent, usually resulting from failure of electric circuit or other electrical components.
	No power	Temporary loss of all electrical power source that result in sudden stop to the whole system operation.
	Low power	Temporary loss of part of the electrical power sources that leads to inability of the system to operate properly.

3. **GUIDEWORDS (Exposure Elements)**

i. IDENTIFY – ability to recognize or select by analysis
ii. OPERATE – function or control of something with respect to a machine or a process
iii. CONTROL – ability to direct a situation, process, etc to desired direction
iv. DISPLAY – ability to show or demonstrate something or particularly data so that it may readily be seen.
v. FUNCTION – ability to operate or work in a proper or particular way as designed

4. **Deviation from design intent based on Guide words:**

IDENTIFY	Fail to identify	Unable to identify
	False identification	Misleading identification
OPERATE	Fail to operate	Unable to operate
	Fail to open	Unable to open
	Fail to close	Unable to close
	Fail to isolate	Unable to isolate
CONTROL	Fail to control	Unable to control
	False control	Misleading control
DISPLAY	Fail to display	Unable to display
	False display	Misleading display
FUNCTION	Fail to function	Unable to function (malfunction)

APPENDIX C

GENERAL RULES OF BOOLEAN ALGEBRA

	Mathematical Symbolism	Engineering Symbolism	Designation
(1a)	$X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$	Commutative Law
(1b)	$X \cup Y = Y \cup X$	$X + Y = Y + X$	
(2a)	$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$ $X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$	Associative Law
(2b)	$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X + (Y + Z) = (X + Y) + Z$	
(3a)	$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$ $X \cdot (Y + Z) = X \cdot Y + X \cdot Z$	Distributive Law
(3b)	$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + Y \cdot Z = (X + Y) \cdot (X + Z)$	
(4a)	$X \cap X = X$	$X \cdot X = X$	Idempotent Law
(4b)	$X \cup X = X$	$X + X = X$	
(5a)	$X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$	Law of Absorption
(5b)	$X \cup (X \cap Y) = X$	$X + X \cdot Y = X$	
(6a)	$X \cap X' = \phi$	$X \cdot X' = \phi$	Complementation
(6b)	$X \cup X' = \Omega = I^*$	$X + X' = \Omega = I$	
(6c)	$(X')' = X$	$(X')' = X$	
(7a)	$(X \cap Y)' = X' \cup Y'$	$(X \cdot Y)' = X' + Y'$	de Morgan's Theorem
(7b)	$(X \cup Y)' = X' \cap Y'$	$(X + Y)' = X' \cdot Y'$	
(8a)	$\phi \cap X = \phi$	$\phi \cdot X = \phi$	Operations with ϕ and Ω
(8b)	$\phi \cup X = X$	$\phi + X = X$	
(8c)	$\Omega \cap X = X$	$\Omega \cdot X = X$	
(8d)	$\Omega \cup X = \Omega$	$\Omega + X = \Omega$	
(8e)	$\phi' = \Omega$	$\phi' = \Omega$	
(8f)	$\Omega' = \phi$	$\Omega' = \phi$	
(9a)	$X \cup (X' \cap Y) = X \cup Y$	$X + X' \cdot Y = X + Y$	These relationships are unnamed but are frequently useful in the reduction process.
(9b)	$X' \cap (X \cup Y') = X' \cap Y' = (X \cup Y)'$	$X' \cdot (X + Y') = X' \cdot Y' = (X + Y)'$	

*The symbol I is often used instead of Ω to designate the Universal Set. In engineering notation Ω is often replaced by 1 and ϕ by 0.

Source: NASA, Fault Tree Handbook with Aerospace Application Version 1.1, August 2002. (Website: *http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf*)

APPENDIX D

SELECTED FAILURE RATE DATA

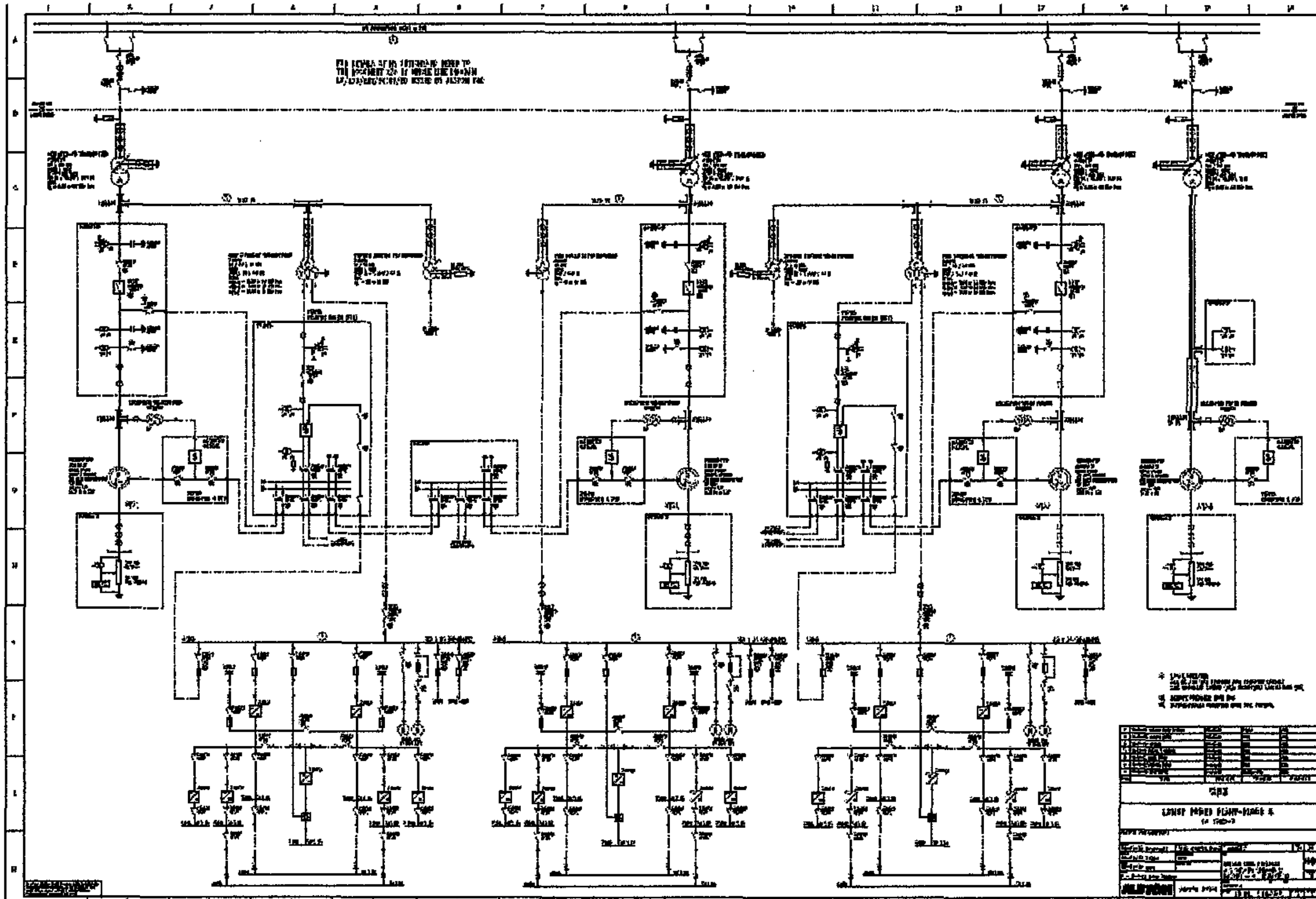
Instrument	Faults/year	R	P	Reference
Annunciators	0.0067452	0.9933	0.0067	Guideline for Process Equipment Reliability Data
Batteries-Lead Acid (No output)	0.01971	0.9805	0.0195	Guideline for Process Equipment Reliability Data
Batteries-Nickel Cadmium (No output)	0.00219876	0.9978	0.0022	Guideline for Process Equipment Reliability Data
Battery Chargers (No electrical output)	0.066576	0.9356	0.0644	Guideline for Process Equipment Reliability Data
Circuit Breakers -AC	0.01533	0.9848	0.0152	Guideline for Process Equipment Reliability Data
Circuit Breakers -DC	0.033288	0.9673	0.0327	Guideline for Process Equipment Reliability Data
Controller	0.29	0.7483	0.2517	Lee's
Controllers-Electronic-Panelboard (Single Loop)	1.7958	0.1660	0.8340	Guideline for Process Equipment Reliability Data
Flame Detectors	3.78432	0.0227	0.9773	Guideline for Process Equipment Reliability Data
Fuses	0.00555384	0.9945	0.0055	Guideline for Process Equipment Reliability Data
Heat Transfer Devices (Catasthropic)	0.272436	0.7615	0.2385	Guideline for Process Equipment Reliability Data
Heat Transfer Devices (Leakage > 1/4")	0.226008	0.7977	0.2023	Guideline for Process Equipment Reliability Data
Indicator lamp	0.044	0.9570	0.0430	Lee's
Indicators-Temperature-Radiation Parameter	2.17248	0.1139	0.8861	Guideline for Process Equipment Reliability Data
Inverters	0.251412	0.7777	0.2223	Guideline for Process Equipment Reliability Data
Motors-AC (Fail to run properly)	0.133152	0.8753	0.1247	Guideline for Process Equipment Reliability Data
Motors-AC-Induction (fail to run properly)	0.028032	0.9724	0.0276	Guideline for Process Equipment Reliability Data

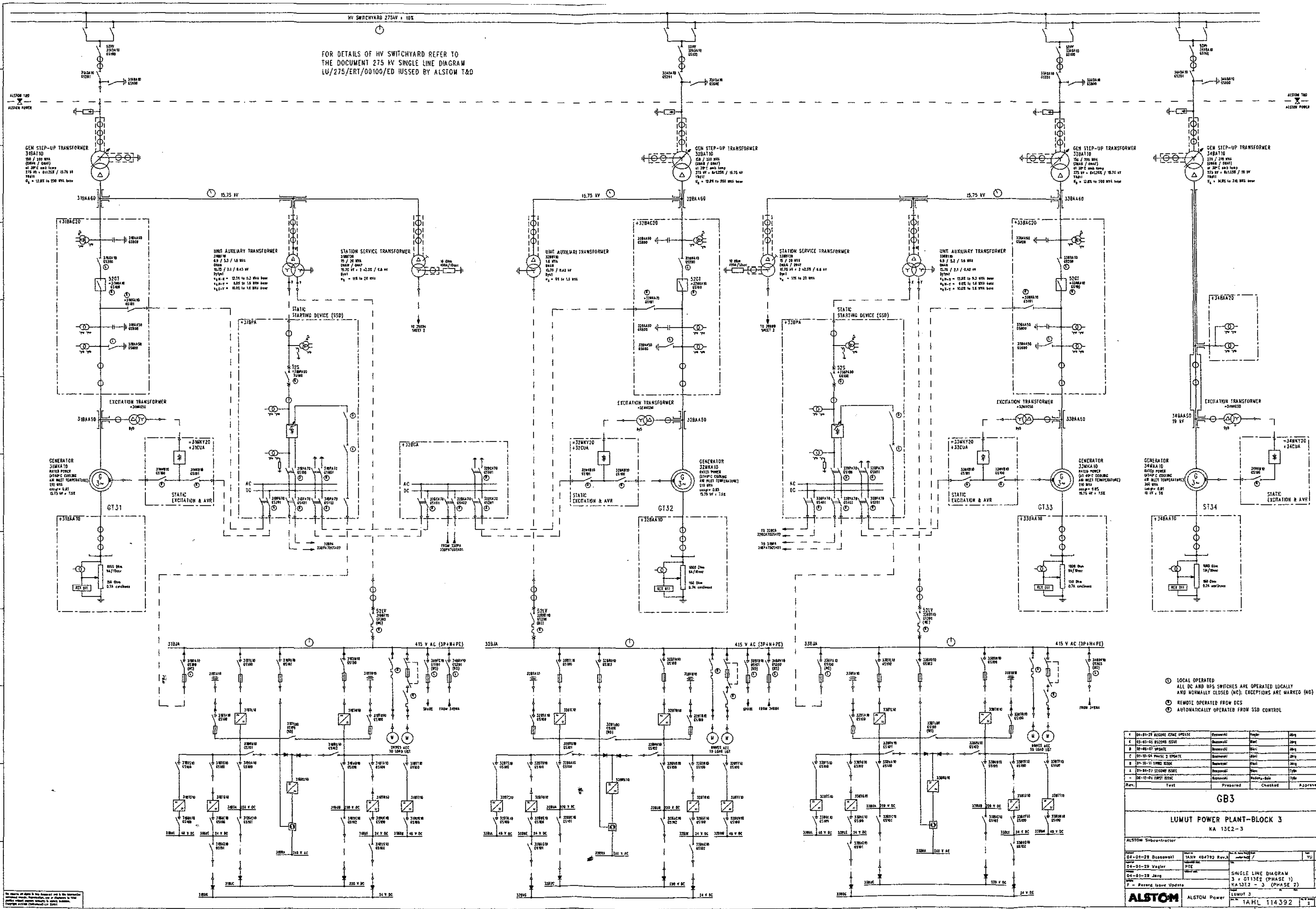
Motors-DC (Fail to run properly)	0.1971	0.8211	0.1789	Guideline for Process Equipment Reliability Data
Recorders	0.219876	0.8026	0.1974	Guideline for Process Equipment Reliability Data
Relays-Protective	0.0167316	0.9834	0.0166	Guideline for Process Equipment Reliability Data
Stepper motor	0.044	0.9570	0.0430	Lee's
Switches-Electric-Flow (Catasthropic)	0.234768	0.7908	0.2092	Guideline for Process Equipment Reliability Data
Switches-Electric-Flow (Fail to function when signalled)	0.036792	0.9639	0.0361	Guideline for Process Equipment Reliability Data
Switches-Electric-Flow (Function w/o signal)	0.0075336	0.9925	0.0075	Guideline for Process Equipment Reliability Data
Switches-Electric-Level (Catastrophic)	0.0152424	0.9849	0.0151	Guideline for Process Equipment Reliability Data
Switches-Electric-Level (Degraded)	0.014892	0.9852	0.0148	Guideline for Process Equipment Reliability Data
Switches-Electric-Level (Fail to function when signalled)	0.0014892	0.9985	0.0015	Guideline for Process Equipment Reliability Data
Switches-Electric-Level (Function w/o signal)	0.008103	0.9919	0.0081	Guideline for Process Equipment Reliability Data
Switches-Electric-Pressure (Catasthropic)	0.434496	0.6476	0.3524	Guideline for Process Equipment Reliability Data
Switches-Electric-Pressure (Fail to function when signalled)	0.003504	0.9965	0.0035	Guideline for Process Equipment Reliability Data
Switches-Electric-Pressure (Function w/o signal)	0.0006132	0.9994	0.0006	Guideline for Process Equipment Reliability Data
Switches-Electric-Speed (Catasthropic)	0.0042048	0.9958	0.0042	Guideline for Process Equipment Reliability Data
Switches-Electric-Speed (Fail to function when signalled)	0.0049932	0.9950	0.0050	Guideline for Process Equipment Reliability Data
Switches-Electric-Speed (Function w/o signal)	0.001314	0.9987	0.0013	Guideline for Process Equipment Reliability Data
Switches-Electric-Temperature (Catasthropic)	0.0199728	0.9802	0.0198	Guideline for Process Equipment Reliability Data
Switches-Electric-Temperature (Fail to function when signalled)	0.029784	0.9707	0.0293	Guideline for Process Equipment Reliability Data

Switches-Electric-Temperature (Function w/o signal)	0.0101616	0.9899	0.0101	Guideline for Process Equipment Reliability Data
Transducers-Current to Pneumatic	0.550128	0.5769	0.4231	Guideline for Process Equipment Reliability Data
Transformers-Power (No output)	0.0221628	0.9781	0.0219	Guideline for Process Equipment Reliability Data
Transformers-Rectifier (No output)	0.0093732	0.9907	0.0093	Guideline for Process Equipment Reliability Data
Transmitters-Differential Pressure	0.574656	0.5629	0.4371	Guideline for Process Equipment Reliability Data
Transmitters-Differential Pressure	1.90968	0.1481	0.8519	Guideline for Process Equipment Reliability Data
Transmitters-Electronic-Level-Capacitance Probe	0.219876	0.8026	0.1974	Guideline for Process Equipment Reliability Data
Transmitters-Pneumatic-Flow	0.95484	0.3849	0.6151	Guideline for Process Equipment Reliability Data
Transmitters-Pneumatic-Flow-Differential Pressure	1.03368	0.3557	0.6443	Guideline for Process Equipment Reliability Data
Transmitters-Pneumatic-Flow-Variable Area	0.843588	0.4302	0.5698	Guideline for Process Equipment Reliability Data
Transmitters-Pneumatic-Level	1.23516	0.2908	0.7092	Guideline for Process Equipment Reliability Data
Transmitters-Pneumatic-Level-Differential Pressure	0.870744	0.4186	0.5814	Guideline for Process Equipment Reliability Data

APPENDIX E

SINGLE LINE DIAGRAM OF LUMUT POWER PLANT (I)





Ⓛ LOCAL OPERATED
ALL DC AND UPS SWITCHES ARE OPERATED LOCALLY
AND NORMALLY CLOSED (NC): EXCEPTIONS ARE MARKED (NO)

Ⓡ REMOTE OPERATED FROM DCS

Ⓐ AUTOMATICALLY OPERATED FROM SSD CONTROL

Rev.	Text	Prepared	Checked	Approved
F	04-01-29 RECORD ISSUE UPDATE	Bossowski	Vogler	Jörg
E	03-03-05 RECORD ISSUE	Bossowski	Bieri	Jörg
D	02-06-07 UPDATE	Bossowski	Bieri	Jörg
C	01-12-04 PHASE 2 UPDATE	Bossowski	Bieri	Jörg
B	01-10-11 THIRD ISSUE	Bossowski	Bieri	Jörg
A	01-04-27 SECOND ISSUE	Bossowski	Bieri	Tylla
-	00-12-06 FIRST ISSUE	Bossowski	Nodeka-Bein	Tylla

GB3

LUMUT POWER PLANT-BLOCK 3

KA 13E2-3

ALSTOM Subcontractor

04-01-29 Bossowski | 1AHV 404792 Rev.A | YU | AO

04-01-29 Vogler | PTE

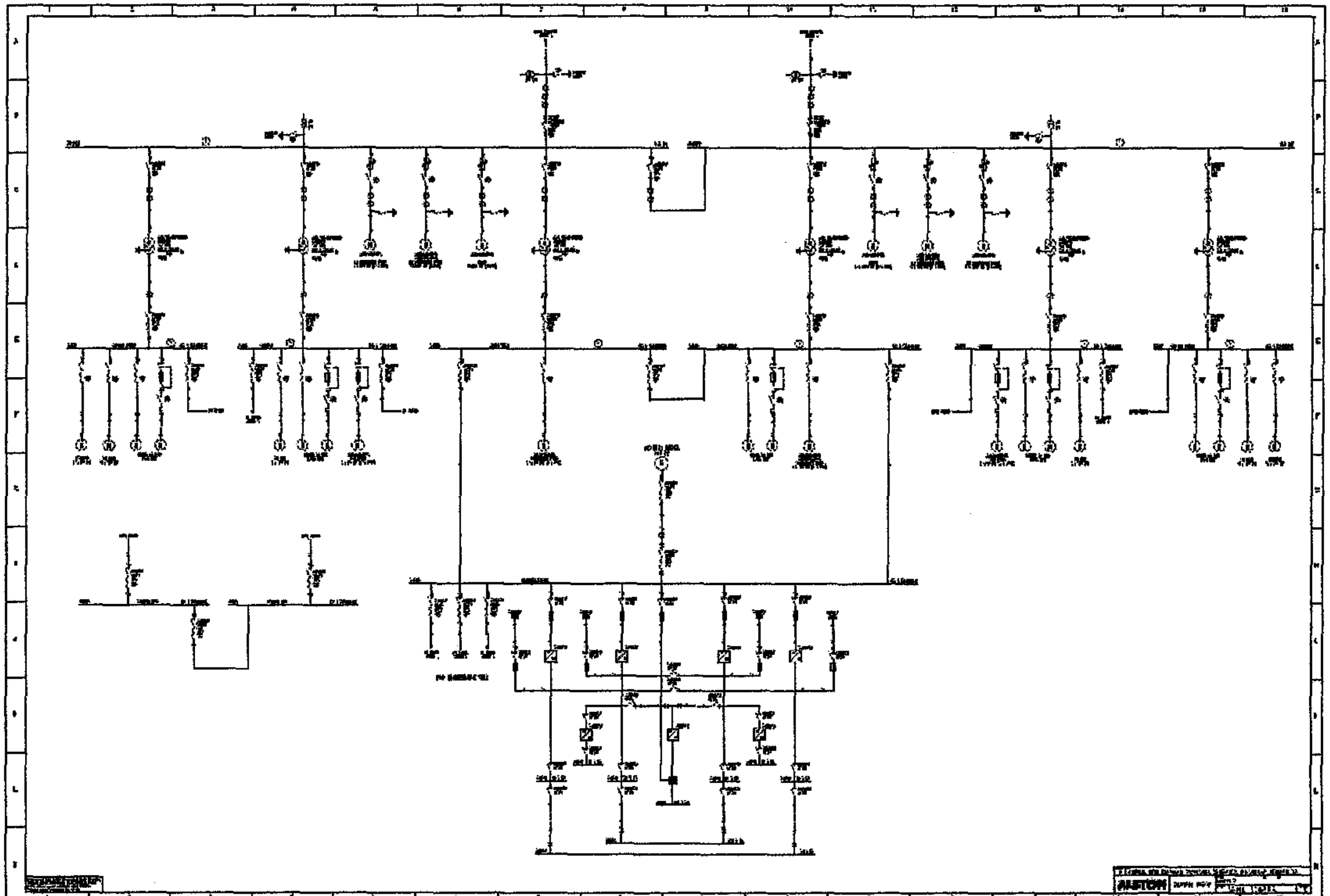
04-01-29 Jörg

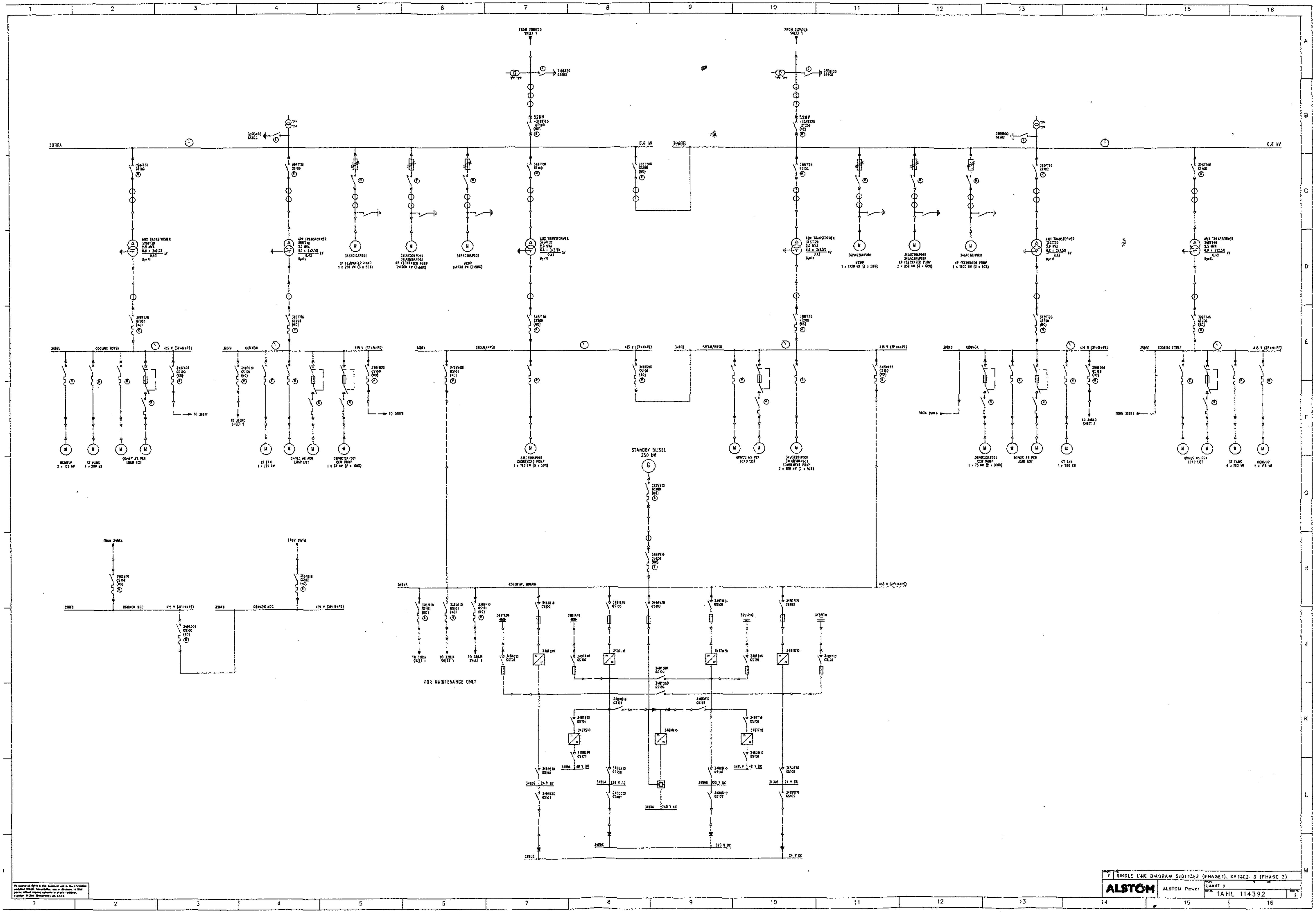
F - Record Issue Update

SINGLE LINE DIAGRAM
3 x GT13E2 (PHASE 1)
KA 13E2 - 3 (PHASE 2)

ALSTOM | ALSTOM Power | LUMUT 3 | 1AHL 114392 | 2 | 1

SINGLE LINE DIAGRAM OF LUMUT POWER PLANT (II)

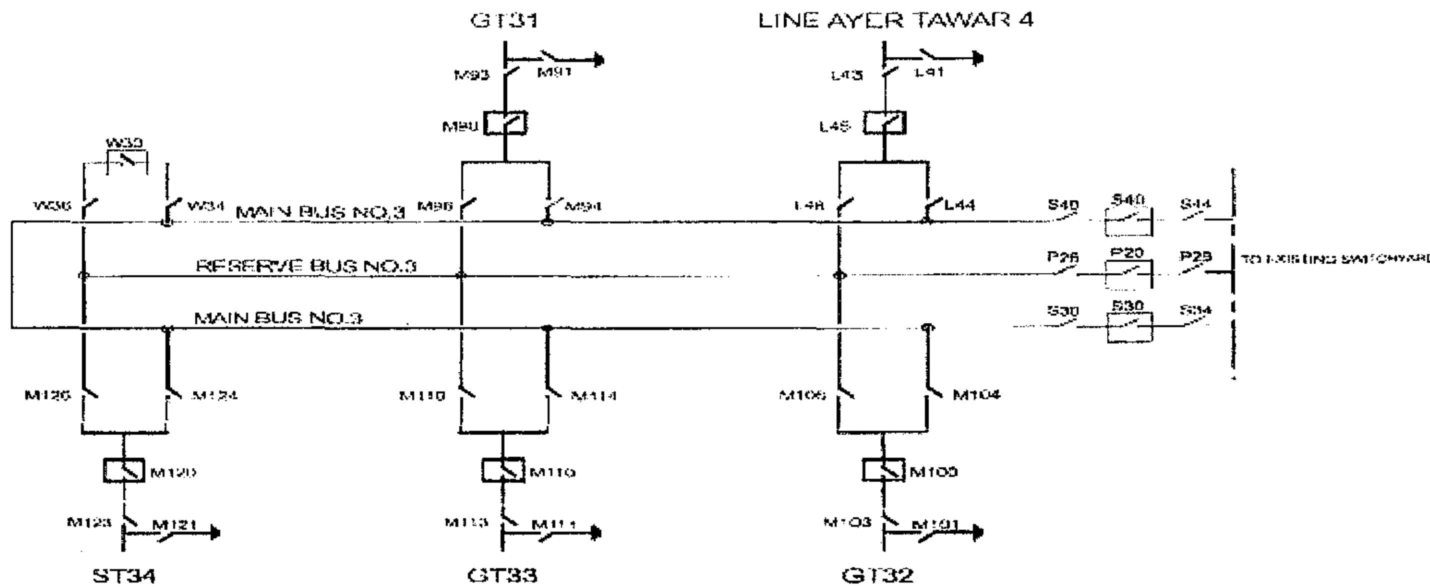




6.6 kV
STANDBY DIESEL
350 kW
ESSENTIAL BOARD
FOR MAINTENANCE ONLY
AUX TRANSFORMER
COOLING TOWER
CONDOR
STEAM/PWSE
415 V (3P+N+PE)
52MV
SINGLE LINE DIAGRAM 3xGT13E2 (PHASE1), KA13E2-3 (PHASE 2)
ALSTOM
ALSTOM Power
LUMUT 3
1AHL 114392

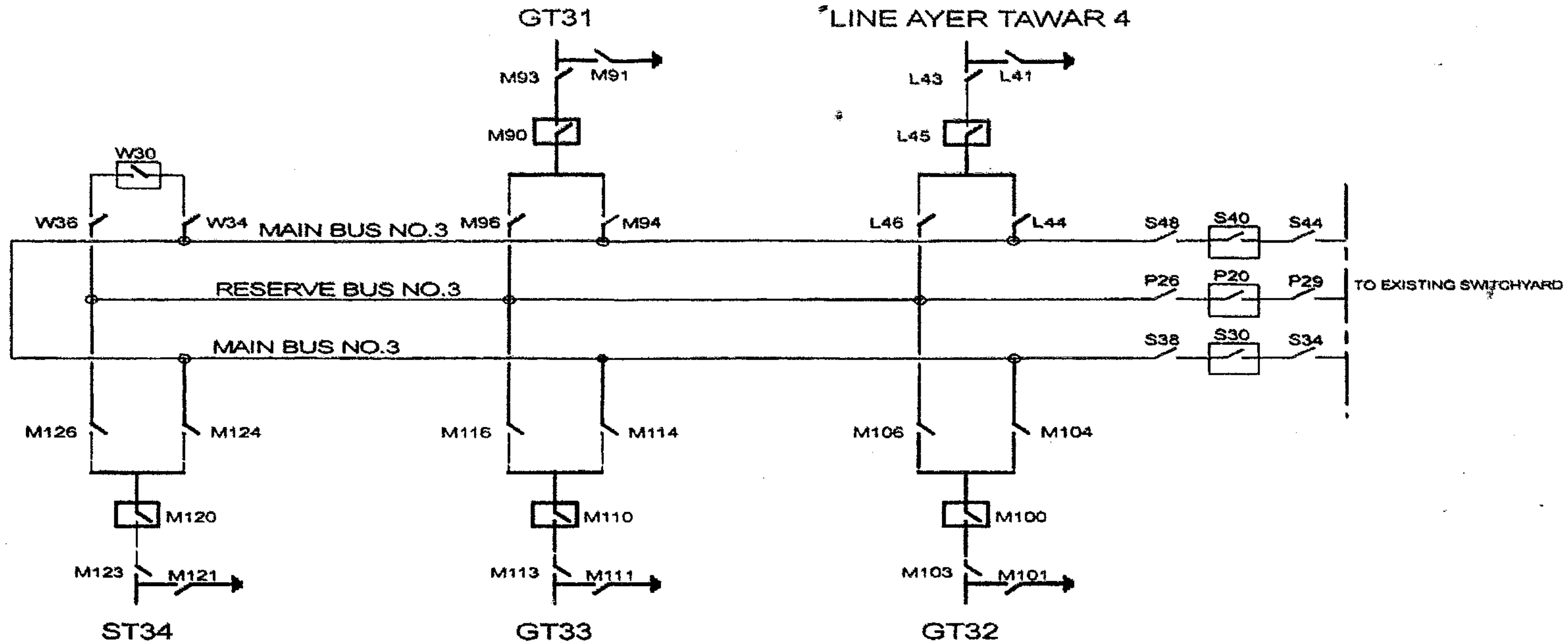
APPENDIX F

SINGLE LINE DIAGRAM OF GAS TURBINE



GT31 : HV. CB. Black Network

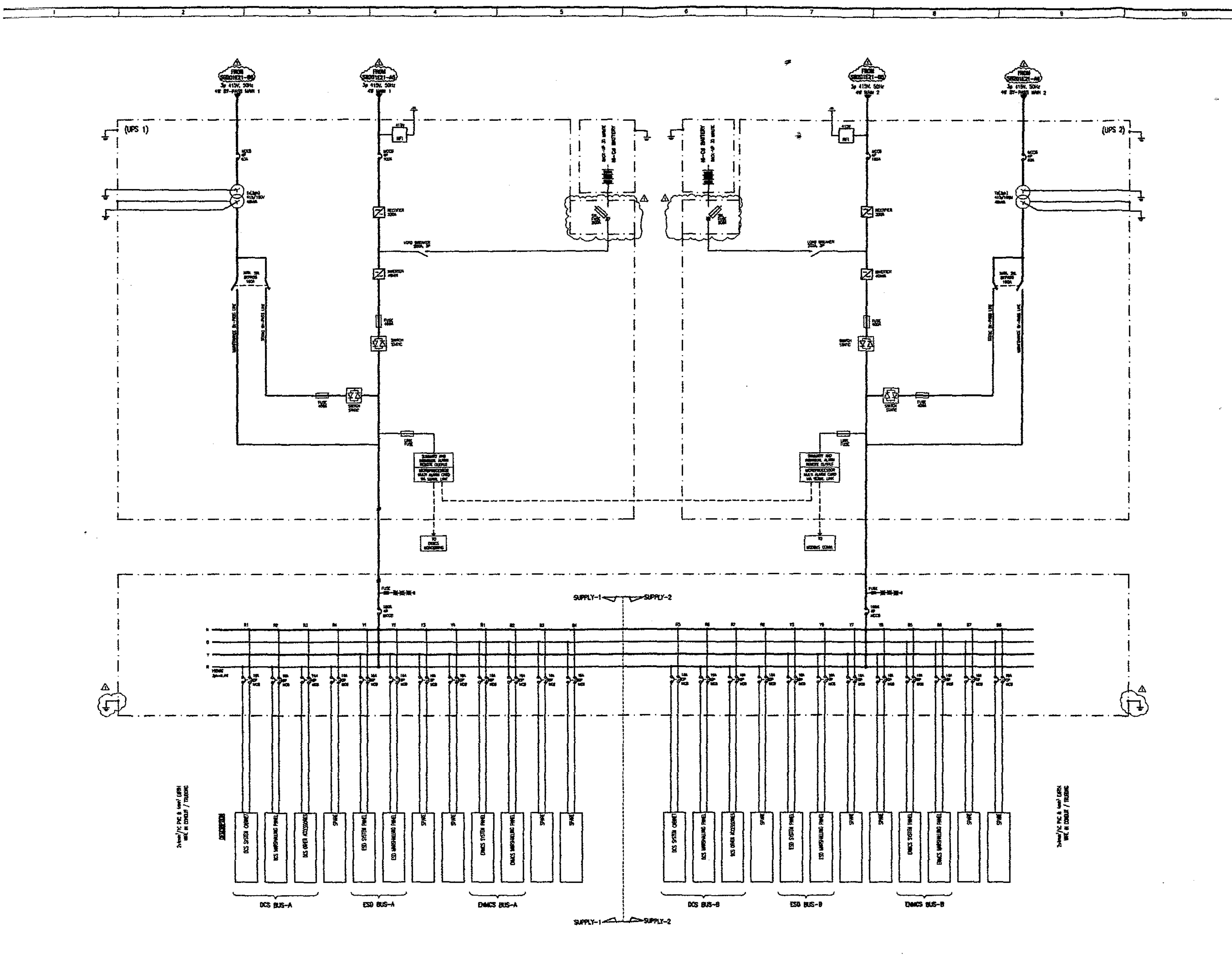
Pre-condition	Equipment **open** status S38,S30,S34 , W36,W30,W34 , S48,S40,S44
	M3 De-energised
	R3 Energised GT31,GT32,GT33,Ayer Tawar 4
	GT31 backfeed via R3 – M96 – M90 – M93
Switching steps	1.GT31 is running and already synchronised through R3 at ____MW via generator circuit breaker
	2.Open M90 by DCS command and GT31 stay in idle
	4.Open M90 > Open M96 > Close M94
	5.Black sync M90 via M94 to dead M3 bus > **Completed Black sync M90 to dead M3 bus**
	6.Open M90 by Power plant > Close W36 > Close W34 > Close W30 energized M3 with TNB power by TNB
	7.HV sync M90 through M94 to M3
	8.TNB normalised HV switchyard Close S48,S44,S40 S38,S34,S30
	9.Completed HV CB sync,Black network



GT31 : HV. CB. Black Network

Pre-condition Equipment **open** status S38,S30,S34 , W36,W30,W34 , S48,S40,S44
M3 De-energised
R3 Energised GT31,GT32,GT33,Ayer Tawar 4
GT31 backfeed via R3 – M96 – M90 – M93

Switching steps 1.GT31 is running and already synchronised through R3 at ____MW via generator circuit breaker
2.Open M90 by DCS command and GT31 stay in idle
4.Open M90 > Open M96 > Close M94
5.Black sync M90 via M94 to dead M3 bus > **Completed Black sync M90 to dead M3 bus**
6.Open M90 by Power plant > Close W36 > Close W34 > Close W30 energized M3 with TNB power by TNB
7.HV sync M90 through M94 to M3
8.TNB normalised HV switchyard Close S48,S44,S40 S38,S34,S30
9.Completed HV CB sync,Black network



Key Plan :

Notes :

1. RFI-BOARD WITH EMC FILTER (RADIO FREQ. INTERFERENCE BOARD)

PFKSB PLANT DEBOTTLENECKING PROJECT
GAS TURBINE COGENERATION SYSTEM

- [ ] APPROVED / REVIEWED
- [ ] APPROVED WITH COMMENT
- [ ] RESUBMIT FOR APPROVAL
- [ ] RESUBMIT FOR REVIEW

NAME	SIGNATURE	TITLE	DATE

REFERENCE DRAWING

DOCUMENT NO.	TITLE

REVISIONS

REV	DESCRIPTION	EPCC CHK	EPCC APP	EPCC DATE	OWNER CHK	OWNER APP	OWNER DATE
1							
0							
B							
A					-	-	-

Client :

PETRONAS FERTILIZER (KEDAH) SDN BHD

EPCC Contractor :

SHINRYO (M) - STEAMLINE (M) CONSORTIUM

Project Title :

PFKSB PLANT DEBOTTLENECKING PROJECT
EPCC OF GAS TURBINE
COGENERATION SYSTEM

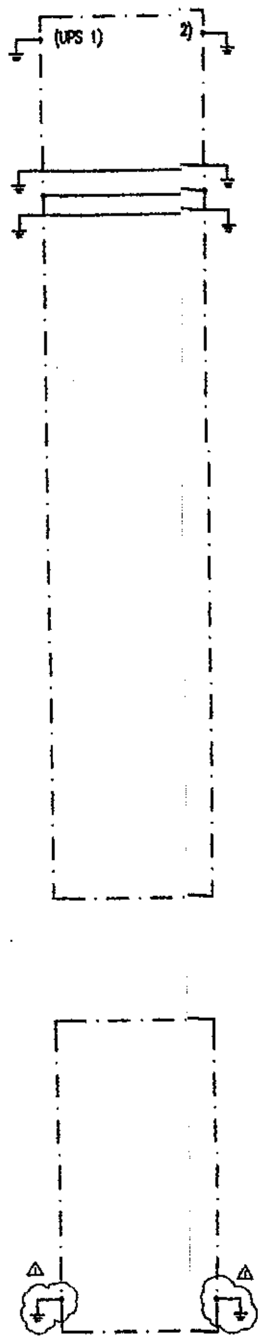
Drawing Title :

ONE LINE DIAGRAM
COGEN SUBSTATION 110V AC
UPS DISTRIBUTION SYSTEM

Scale :	N.T.S	Date :	09 OCT. 2008
Drawn By :	AZIZI	Design By :	KC.TAN
Cad File :	DPFK5970009IR1		
Drawing Number :	D-PFK-59-70-0091	Rev :	1

DISTRIBUTION	
PFK	
PD	
PM	
CTRL & S M	
ENG & C M	
PRO & C M	
CIVIL	
PIPING	
ELECT	
INST	
MECH UNIT/EQU	
ROTATING	
PROCESS UNIT	
COST CTRL	
DOC & SCHE	
PROCU & CONT	
QA/QC	
HSE	
COPY	
TOTAL	

1	2	10



Key Plan :

Notes :

1. RFI-BOARD WITH EMC FILTER (RADIO FREQ. INTERFERENCE BOARD)

PFKSB PLANT DEBOTTLENECKING PROJECT GAS TURBINE COGENERATION SYSTEM

- [ ] APPROVED / REVIEWED
- [ ] APPROVED WITH COMMENT
- [ ] RESUBMIT FOR APPROVAL
- [ ] RESUBMIT FOR REVIEW

NAME	SIGNATURE	TITLE	DATE

DOCUMENT NO.	TITLE
[illegible]	[illegible]
	[illegible]
[illegible]	[illegible]

REFERENCE DRAWING

		EPCC			OWNER		
REV	DESCRIPTION	CHK	APP	DATE	CHK	APP	DATE
1	[illegible]	[illegible]	[illegible]	[illegible]			
0	[illegible]	[illegible]	[illegible]	[illegible]			
B	[illegible]	[illegible]	[illegible]	[illegible]	-	-	-
A	[illegible]	[illegible]	[illegible]	[illegible]	-	-	-

REVISIONS

Client :

PETRONAS FERTILIZER (KEDAH) SDN BHD

EPCC Contractor :

SHINRYO (M) - STEAMLINE (M)
(95403-A) (463912-K)
CONSORTIUM

Unit 24.02, 24th Floor,
Menara [illegible],
Jalan Sultan Ismail,
50250 Kuala Lumpur
Tel. : 03-2144 8066
Fax : 03-2142 8955

Project Title :

PFKSB PLANT DEBOTTLENECKING PROJECT
EPCC OF GAS TURBINE
COGENERATION SYSTEM

Drawing Title :

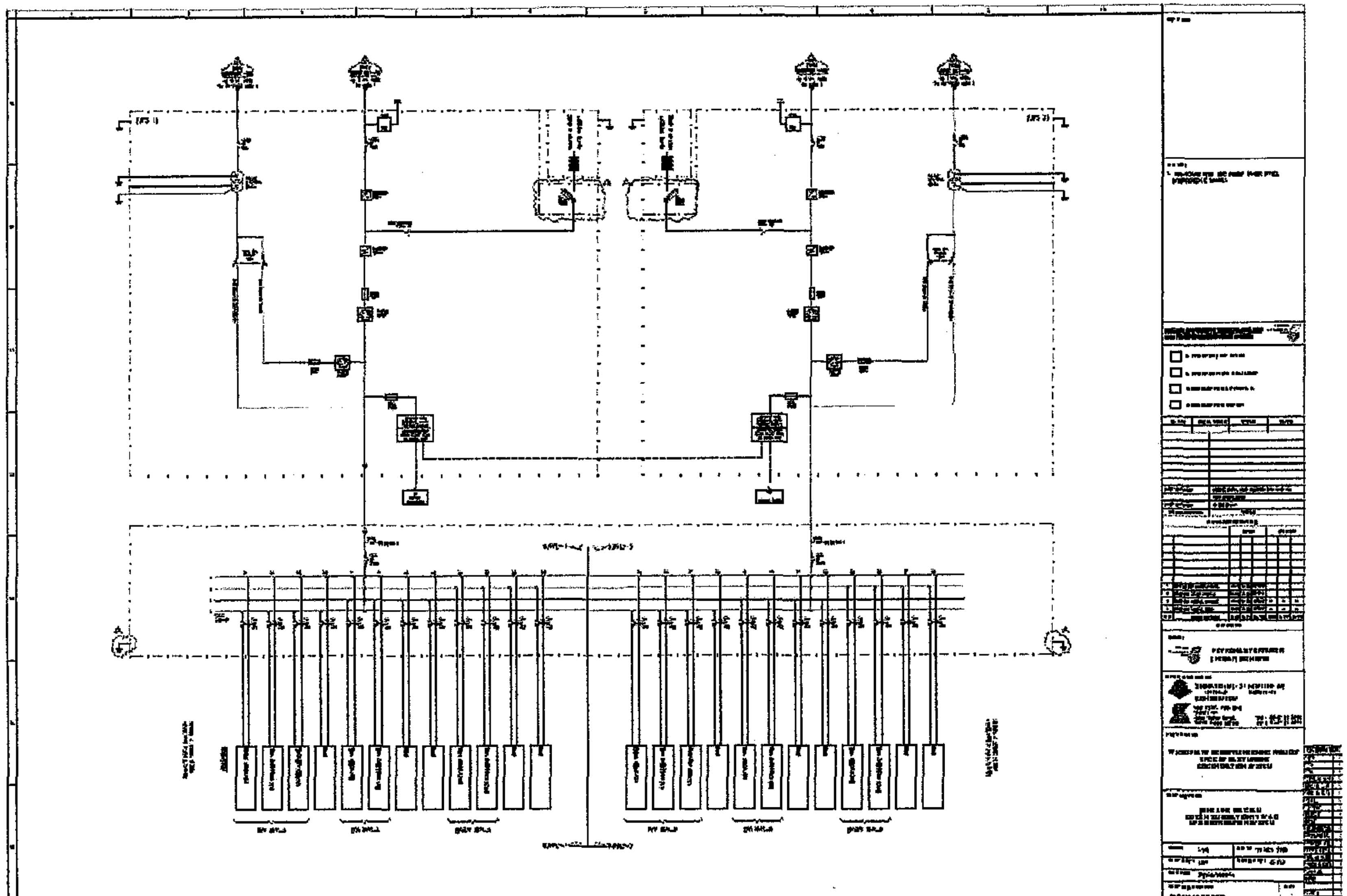
ONE LINE DIAGRAM
COGEN SUBSTATION 110V AC
UPS DISTRIBUTION SYSTEM

Scale : N.T.S	Date : 09 OCT. 2008
Drawn By : AZIR	Design By : KC.TAN
Cad File : DPFK5970009IR1	
Drawing Number :	Rev.

DISTRIBUTION	
PFK	
PD	
PM	
CTRL & S M	
ENG & C M	
PRO & C M	
CIVIL	
PIPING	
ELECT	
INST	
MECH UIL/OSG	
ROTATING	
PROCESS UIL	
COST CTRL	
DOC & SCHE	
PROCU & CONT	
QA/QC	
HSE	

APPENDIX G

SINGLE LINE DIAGRAM OF AC UPS OF PFK



APPENDIX H

GENERAL REQUIREMENTS FOR AC UPS SYSTEM

Construction Requirements

- All batteries shall be of the nickel-cadmium (Nicd) type.
- The nominal output of the DC UPS system shall be 110V DC supply.
- The units shall be provided with an input harmonic filter and surge suppression device, as well as output filter.
- Name, identification, instruction, and wiring plates:
    - All name, identification, instruction and wiring plates shall be engraved with indelible inscriptions in the English language. Labels shall be of sufficient size to provide easy reading from normal operating & maintenance positions. Labels shall be provided to indicate the main functions of each service and control equipment.
    - Plates mounted on the outside of the equipment shall be fixed of durable self-threading screws or pop-rivets.
    - All labels except danger/ warning labels fixed on the surface of panel / equipment shall be engraved black lettering on white plastic material.
    - Warning plate(s) or caution notice(s) shall be installed, identifying the danger point(s). This shall be in the compartment and/ or on the outside of the assembly. DANGER/WARNING Labels shall be engraved with RED colour on white plastic material.
    - Instruction Plate shall be provided wherever applicable and it shall be, if possible, in a pictorial manner.

- Circuit labels shall be provided to allow easy and clear identification of the circuit from the front and back with the access doors open or closed. All trip wiring shall be identified with a red ferrule marked with the letter "T".
- Each item of the equipment shall have the manufacturer's rating plate with catalogues and / or serial nos. and other relevant information.

- The enclosure shall provide a degree of protection of IP 41.
- Ingress Protection : IP41 (external), IP20 (Internal).
- Cable Entry : Bottom entry.
- Enclosure : Free floor-standing sheet steel cubicle Rusted inhibitor and chemical resistant epoxy paint. Metal shall be electro galvanized type.
- Colour codes for all elec. equipment
  - Indoor equipment : RAL 7035 (Light grey)
- Battery Rack construction : Free Floor standing steel racks with diagonal earthing bossed, acid resistant, no hygroscopic. Leak reservoir under the battery stand.
- Battery Rack finishing : Black Epoxy coated.

3.2.3 Site/Service Conditions

The DC UPS unit shall be located inside a freely ventilated air-conditioned room. However all equipment shall be capable of operation occasion under following condition.

- Maximum ambient air temperature : 40 °C

- Average DC UPS room air temperature : 20 °C to 25 °C
- Minimum ambient air temperature : 5 °C
- Relative humidity not exceeding : 90%
- Altitude not exceeding : 1000 m

The sound pressure level measured at 1 m distance from the DC UPS, at any position, shall not exceed 70dB(A) at any load between zero and the rated output of the unit.

The nominal system input voltage and frequency variations shall be as follows:

- Supply Voltage : 3 Phase 415V
- Supply Frequency : 50 HZ
- Voltage Variations : Voltage ±10%
- Frequency Variations : Frequency ± 5%

The nominal output of 110V DC UPS system shall be 110V DC 50Hz supply.

Source: PFKSB, PFKSB Plant Debottlenecking Project EPCC Of Gas Turbine Cogeneration System