



SPE 107012-PP

Petroleum Facilities Reliability Assessment Model

Luis Palmieri, Pablo Alonso, Adrián Moreno/Repsol YPF

Copyright 2007, Society of Petroleum Engineers

This paper was prepared for presentation at the 2007 SPE Latin American and Caribbean Petroleum Engineering Conference held in Buenos Aires, Argentina, 15–18 April 2007.

This paper was selected for presentation by an SPE Program Committee following review of information contained in an abstract submitted by the author(s). Contents of the paper, as presented, have not been reviewed by the Society of Petroleum Engineers and are subject to correction by the author(s). The material, as presented, does not necessarily reflect any position of the Society of Petroleum Engineers, its officers, or members. Papers presented at SPE meetings are subject to publication review by Editorial Committees of the Society of Petroleum Engineers. Electronic reproduction, distribution, or storage of any part of this paper for commercial purposes without the written consent of the Society of Petroleum Engineers is prohibited. Permission to reproduce in print is restricted to an abstract of not more than 300 words; illustrations may not be copied. The abstract must contain conspicuous acknowledgment of where and by whom the paper was presented. Write Librarian, SPE, P.O. Box 833836, Richardson, Texas 75083-3836 U.S.A., fax 01-972-952-9435.

Abstract

The purpose of this paper is to create a calculation model to estimate the operation failure probability of an oil production facility, to guarantee an operation without accidents, without dangerous failures, observing the safety and environment policy established by the company. The facility operation is considered successful when it can carry out the functions it was design for.

Once the failure rate has been obtained, the system reliability level is obtained. The quantification of the success or failure is carried out through the application of the Failure Tree technique. The Safety and Operativity systems have been separately analyzed; taking into account that each of them has to be considered independently.

The model was used in the calculation of facility reliability in an oil field. ⁽¹⁾

Introduction

In the current maintenance management, the reliability concept has the purpose of creating maintenance plans based on technical criteria that assure the operation of the assets in the different operating contexts.

These concepts are well used in upstream operations, and that is the reason why this model has been developed to incorporate them on the facilities and equipment which, up to now, have been maintained with programs based on strict, periodic maintenance plans, which were made based on personal and manufacturer's experience, or working with the breakage.

Although the typical conditions of this type of industry, and of upstream in particular, make us believe that it would be pointless to work with mathematical and statistical models of calculus, reality shows us that safety and environment conditions currently adopted by companies, governmental

regulations and maintenance cost optimization asked for to the operating sectors are the ones that really provide support to the developed calculus.

This developed calculus combines the concepts that are then indicated in such way that they provide a global view of how to obtain the reliability degree in both operation and safety of an upstream oil industry system.

Statement of Theory and Definitions

System: It is a deterministic entity which consists of a collection of discreet elements that interact.

System limit: there are three limits: external limit, internal limit and resolution limit.

External Limit: It is defined by the parts or aspects of the system we want to develop.

Internal Limit: It is defined by the selection of the subsystems we want to divide the system into for analyses purposes.

Resolution Limit: It is the level of a lower subsystem we want to analyze. Fig.1

Safety vs. Control: The safety systems take action when the equipment and process variables reach values out of their safety range. This situation can be due to several reasons, equipment failure (pipeline breakage, stuck valves) abnormal process conditions (abnormal gas rate, low temperatures) and failure of the control equipment itself, operator's mistakes when working with the process in manual, etc.

A particular situation to take into account is the normal or emergency equipment start-up, since the critical variables can move out of the safety range.

The international standards indicate in a compulsory way that the safety systems must be independent of the process control systems, to avoid the failure common causes. The International standard IEC 61508 / 61511 deals with the reliability of the Systems related to safety, linked to the process risks. And only the dangerous failure mode is used. Simultaneous satisfaction is given to the process safety and continuity.

It has to be taken into account that the unexpected interruptions of the process are dangerous in themselves, over and above the economic losses that are generated.

Complying with the Reliability that the standard demands is a necessary but not sufficient condition, thus it has to be verified that the selected safety system guarantees a reliability value to the non interruption of the sufficiently reasonable process ⁽²⁾

Reliability: Ability of a system to carry out the required functions, under specific conditions, during a established period of time. It is measured as the probability that a system is operative without failure during the mission period of time.

Failure: Situation in which the equipment or system stops carrying out the function(s) for which it was designed or installed.

Failure Mode: It is the effect through which a failure becomes apparent. The failure mode can be divided into two main types:

- a) The change of the demanded or required state is not achieved.
- b) Unwanted change in the conditions or state.

Dangerous failure: Failure to the assigned function, undetectable failure. It is only detectable through inspection. The dangerous failure prevents the safety system from performing in the case its action is required, i.e. the system is not available.

Safe failure: Failure which is caused by the safe action of the system.

Failure On Demand Probability: It occurs when the protection system is not available.

Failure Rate: It is the function that tells us the number of failures that an item is going to have during its life span.

Failure Probability Distribution: It is the mathematical expression that models how the failures are distributed through time (for example, exponential, lognormal, Weibull, Poisson, etc distribution.)

Failure Tree: Systematic method to obtain information of a system. This information can be used for the complex decision-making process.

It is in itself a graphic model of the several failure parallel and sequential combinations which will result in the occurrence of the predefined unwanted event.

Although it is a mainly qualitative model, it can be quantitatively evaluated.

An unwanted event represents the upper point in a failure tree diagram, which provides the method to determine the causes of reaching that point.

This event is the most important and has to be carefully determined. The failure tree leads to a final event, which corresponds to a specific failure mode, and all the events that contribute have to follow that failure mode (Fig.2) ⁽³⁾

Operational context: It is the environment in which a piece of equipment or system is working. This environment is very important since it has influence on the failures the system may have. In other words, the same system can fail in different ways according to the context in which it is operating.

Maintainable item: It is the set of parts that represents the lowest inspection level during maintenance.

Homogeneous Sample: It consists of identical maintainable

items in operational contexts and of an identical environment.

Multiple Sample: The failure rate varies between the different operational and environmental contexts, and each of them represents a sample ⁽⁴⁾.

Method Descriptions and Results

The proposed method is summarized in the flow diagram shown in the Fig.3.

This diagram starts with the system general definition in which the limits, subsystems, components, maintainable items, etc are set. The operational context is also defined.

Taking into account that there can be safety systems involved, these shall be analyzed separately using the process established by the standard IEC 61508 (Fig. 6 and 7) ⁽⁵⁾ and the Risk Quantification is evaluated by:

$$FPD = \frac{F_t}{F_{np}}$$

$$FPD = \lambda_p \times T_{test}$$

$$F_t = FPD \times T_{test} \times D$$

After that, the system functions shall be established, identifying all the failures to the established functions. Each identified failure shall be associated to the specific failure mode that affects the assigned function ⁽⁶⁾. The frame of reference to identify these specific failure modes will be the standard ISO 14224. ⁽⁷⁾

Once all the information above has been defined, the construction of the failure tree shall begin, which is a deductive process in which the following steps are going to be taken:

1. Proposal of the specific state "state of failure".
1. Systematic linkage of basic failures that contribute to occurrence of the unwanted event.

Given this basic structure, we are ready to continue with the quantitative stage of this method.

For doing so, some data is needed. Based on the availability of such data, we have to choose between the analysis with our own data (Fig.5) or data obtained from OREDA DATA BANK (Fig.4).

As shown in Fig.4, Oreda Data Bank requires to determine the type of samples being analyzed (multiple or homogeneous), in order to determine the table column from which the data is going to be obtained.

Multiple Sample: The column MEAN, which is the average of the failure rate that the estimator OREDA establishes, is going to be used.

Homogeneous sample: The column "η/τ" is going to be used.

Once the column has been determined, the line to be used

shall be selected, taking into account the failure mode specified in the analysis.

If there is no specific failure mode observed, the line ALL MODES is going to be used, thus obtaining the failure rate of the analyzed component.

After obtaining all the failure rates of the components that generate events in the failure tree, the logic of the tree is going to be applied and the system final failure rate is going to be determined. ⁽⁴⁾

A distribution of the constant failure rate is accepted. This distribution is sufficiently representative of the reality based on the following:

1 Different combined distributions for a variety of components follow an exponential law. This is mathematically demonstrable.

2 The repair of failures in a specific piece of equipment tends to produce a constant failure rate.

3 When trying to compare reliabilities between pieces of equipment (relative reliability), the distribution with constant failure rate is excellent. ⁽²⁾

In order to calculate the system reliability, the next equation is going to be used.

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

Reliability Exponential Function

In the Fig.5, the steps to be followed are shown if using available information in our own databases.

A big group of data (more than 20), from a statistical point of view, can be used to perform a failure probability distribution analysis that helps to select the most appropriate distribution. With less than 20 data, Weibayes is going to be used as the failure probability distribution, in which parameter β (form factor) shall be estimated according to the age of the analyzed component and the failure mode specified, resulting in a Weibull analysis, and the reliability value is determined according to the next equation ⁽⁸⁾

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^\beta}$$

Weibull Reliability Function

When having more than 20 data, this group will adjust to one of the following failure probability distribution types: Weibull, lognormal, normal, exponential, and the distribution adopted will be the one in which the smallest error in the adjustment is obtained.

In the case in which the adjustment is not acceptable, the data used shall be revised in order to detect possible problems of mixture and/or competence of the failure modes, batch of data. If any of these problems arise, other statistical methods, from which the reliability value can be determined, shall be applied.

If it is not possible to determine the data problem, it shall be assumed that these are not reliable enough; therefore, we

should proceed according to what the flow diagram of the Fig.4 indicates.

Once the distributions that best adjust to each failure mode have been determined, the reliabilities are going to be calculated according the nexts equations: ^{(9) (10)}

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

Reliability Exponential Function

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^\beta}$$

Weibull Reliability Function

$$R(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_t^\infty e^{-\left[\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2\right]} dt$$

Normal Reliability Function

$$R(t) = \int_T^\infty \frac{1}{\sigma_T\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma_T}\right)^2} dt$$

LogNormal Reliability Function

After obtaining all the reliability values of each component, the failure tree logic previously built shall be applied, and the system final reliability will be determined according to the next equations: ⁽¹⁰⁾

$$R_{System} = \prod_i^n R_i$$

Serie System Reliability

$$R_{System} = \prod_i^n F_i = 1 - \prod_i^n (1 - R_i)$$

Parallel System Reliability

Conclusions

This model was used to calculate the reliability of an oil standardized battery. The result obtained was used to identify improvement opportunities, and carry out reengineering in the subsystems that are part of the battery and have higher impact on the calculated value of the total reliability.

Acknowledgments

Professor Eng. Héctor Ecay, Austral Buenos Aires University, for his invaluable help in our analysis and for being our mentor in Reliability Engineering.

Austral University, Buenos Aires, Argentina represented by the Engineers Pedro Univaso and Roberto Bottini, who were part of our training as maintenance engineers.

Maria Amelia Lucero and Andrés Bateman for their assistance and collaboration in this project.

Repsol YPF, for its help during the project.

Nomenclature

R(t) = Reliability Function

F(t) = Unreliability function

i, n = indexes
 FPD = Failure Probability on Demand
 λ = Failure rate
 SIL = Safety Integrity Level (failures/year)
 F_t = Tolerable frequency of the unwanted event (accidents/year)
 H = Hazard rate
 η = Number of failures
 τ = time in service.
 F_{np} : Accident Frequency without protection
 λ_p : Dangerous Failure Rate
 T_{test} : Time between test (year/test)
 D: Demand (demand/year)

10. Jardine, A. and Tsang, A., "Maintenance, Replacement and Reliability", Taylor and Francis Group.

References

1. Palmieri, F., Alonso, P. and Moreno, A. "Standart Facility Reliability Analysis", paper IAPG presented at the IAPG 4th Quality in Maintenance Conference, Neuquén, Argentina, April 2006.
2. Ecay, H.E.J., "Reliability, Maintainability and Risk", Module 2 of Maintenance engineering and management program, Austral University, Buenos Aires, Argentina, (2004)
3. Haasl, D.F., Roberts, N., Vesely, W. and Goldberg, F., "Fault Tree Handbook", NUREG 0492, U.S. Nuclear Regulatory Commission, Washington DC, USA (January 1981)
4. SINTEF Industrial Management, "Offshore Reliability Data", 4th Edition, Oreda Participans, Det Norske Veritas, Norway (2000)
5. IEC 61508, "International Standart", first edition, 1998
6. Moubray, J., "Reliability-centred maintenance (RCM)", spanish edition, Aladon LLC, North Carolina, USA (2004)
7. ISO 14224, "International Standart", first edition, 1999
8. Avernethy, R., "The New Weibull Handbook, second edition, (1996)
9. Duffuaa, S., Raouf, A. and Campbell, J.D., "Maintenance System (planning and control), first edition, Limusa Wiley, Mexico DF (2000)

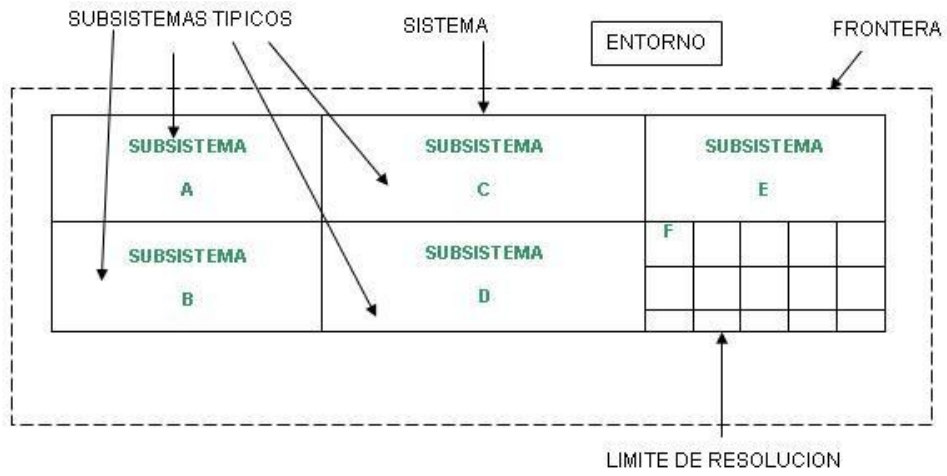


Figure 1 – System Flow Diagram

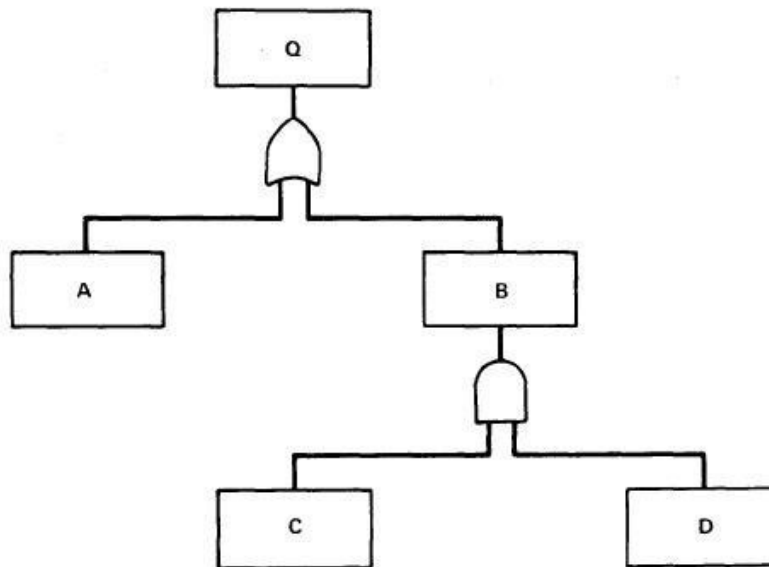


Figure 2 – Failure Tree Example

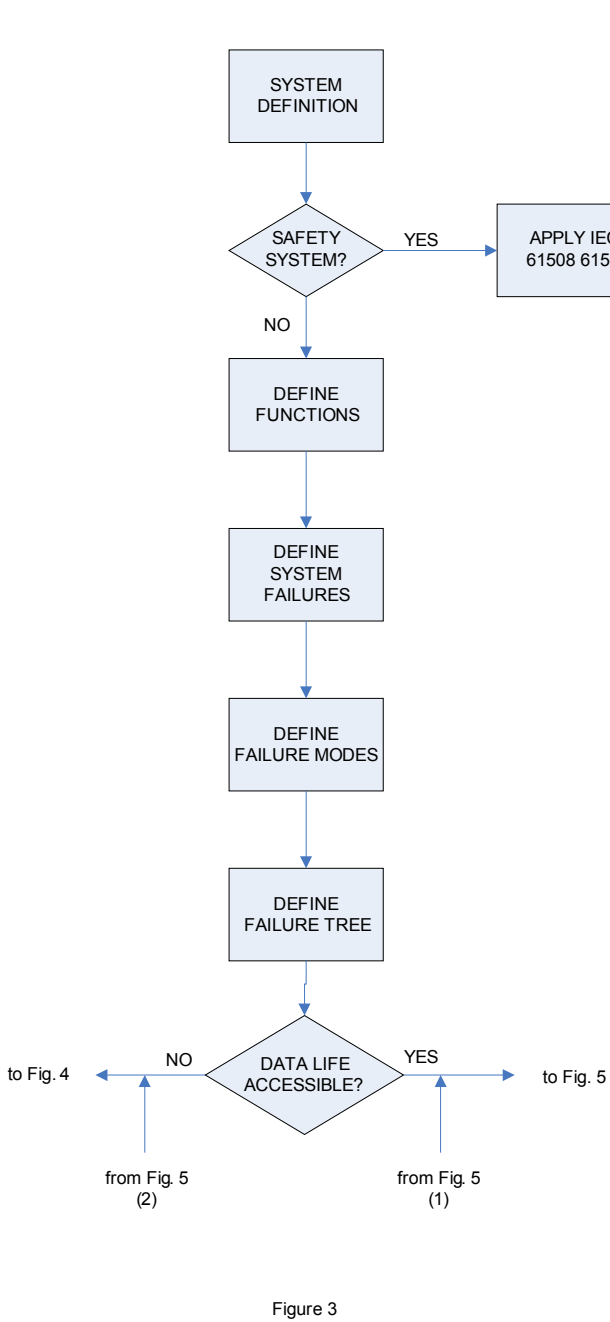


Figure 3 – General Flow Diagram

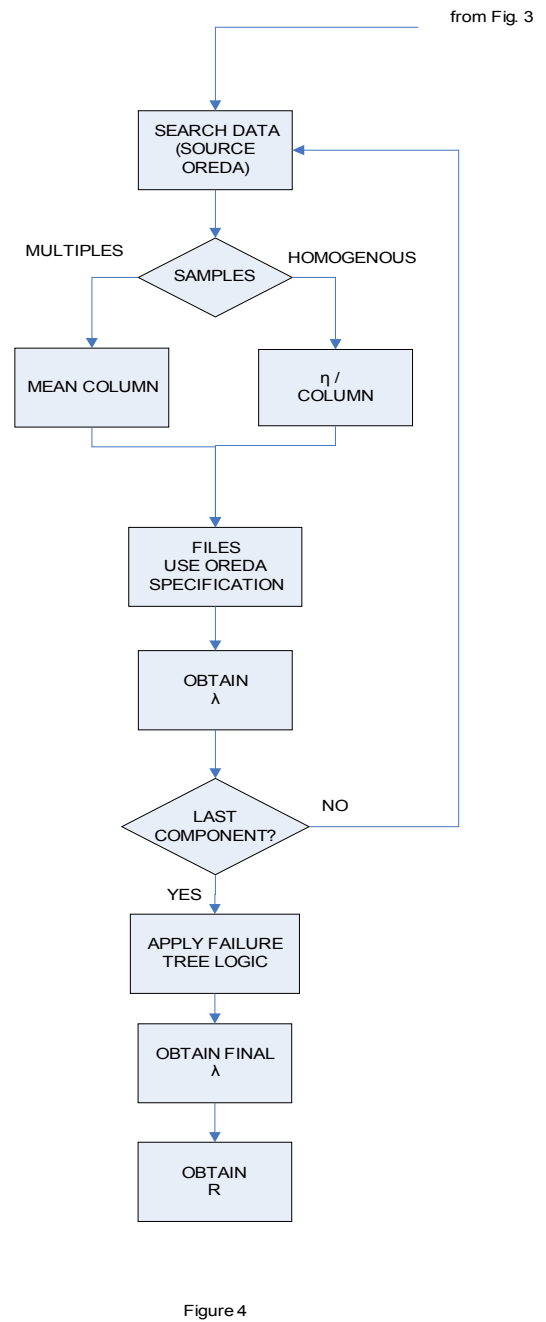


Figure 4 – Flow Diagram Branch Oreda

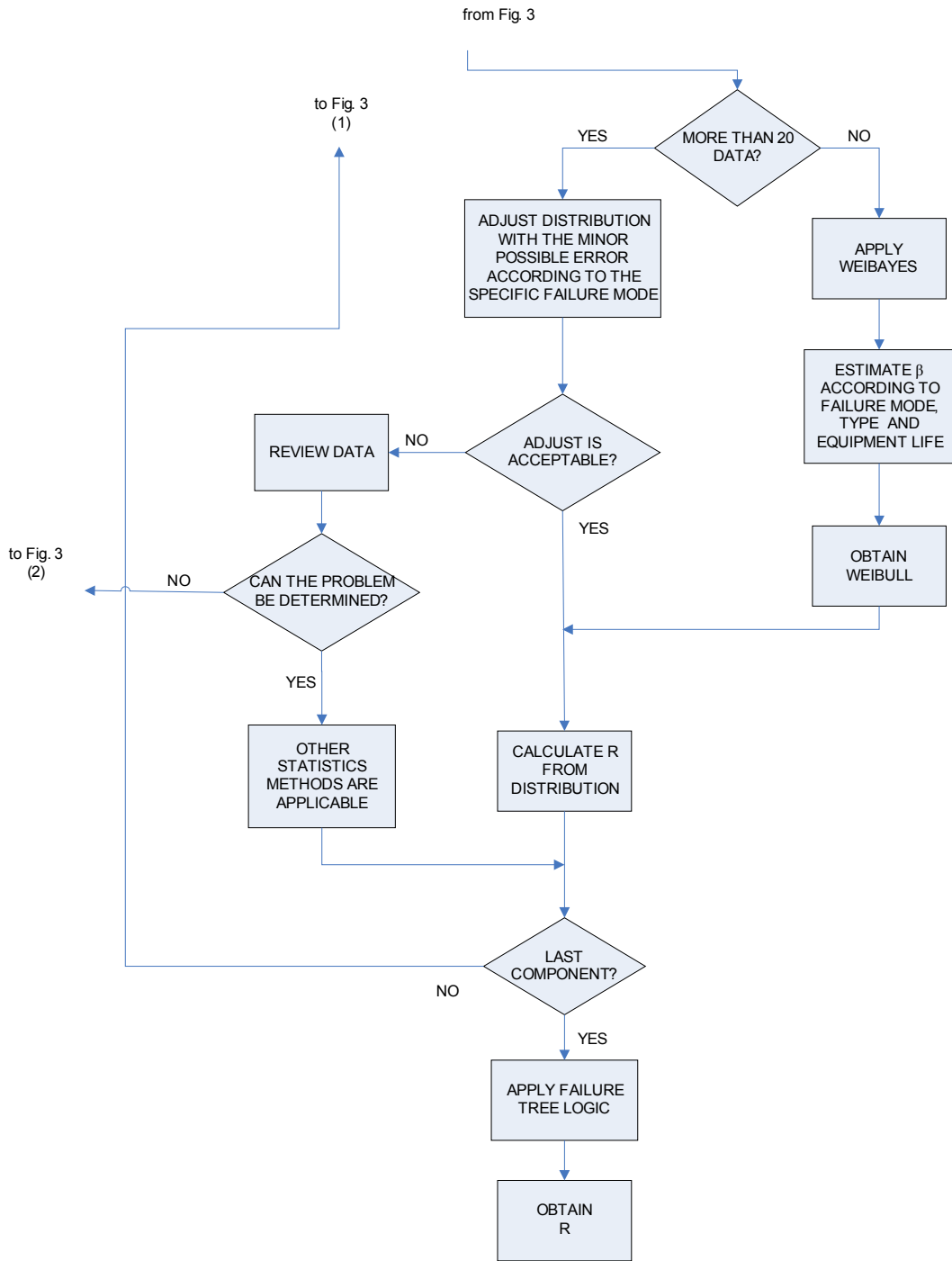


Figure 5

Figure 5 – Flow Diagram Branch own company’s data

Risk Graph Method

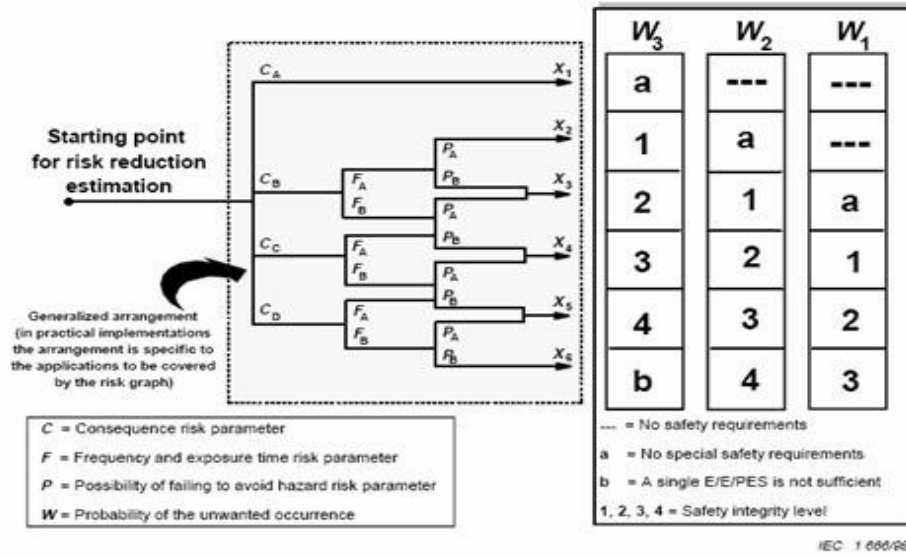


Figure 6 - IEC 61508

Severity Matrix Method

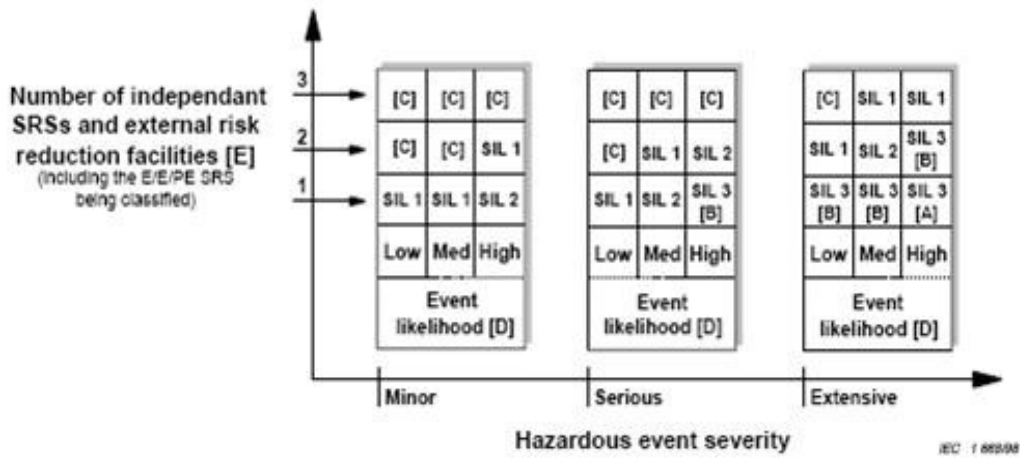


Figure 7 - IEC 61508