Assessing systems reliability: a Probabilistic Risk Assessment (PRA) approach

This item was submitted to Loughborough University’s Institutional Repository by the/an author.


Additional Information:

- This is a conference paper. Further details of the conference are available at: http://www.lboro.ac.uk/departments/tt/arts/index.html

Metadata Record: https://dspace.lboro.ac.uk/2134/5391

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by-nc-nd/2.5/
Assessing Systems Reliability: A Probabilistic Risk Assessment (PRA) Approach

Maged Morcos
Department of Electronic and Electrical Engineering, Systems Engineering Innovation Centre (SEIC), Loughborough University, Loughborough, UK

Abstract

Assessing the reliability performance of complex system involves dealing with events whose occurrence cannot be predicted easily. Not only a good descriptive procedure of the system's components is required but the solution requires some means by which the likelihood of the events can be expressed in terms of quantitative methods. This can be done by adopting a probabilistic risk and reliability assessment method to assess system behaviour. This requires enhancing the reliability analysis with a probabilistic risk analysis technique. The procedure of integration suggested in this work is called Probabilistic Risk Analysis [PRA]. It involves: 1) Identification of the potential events of failures and their modes of failures. 2) Estimation of the consequences of these failures on the total system. 3) Estimation of the probability of occurrence of each event of failure. 4) Comparison of the results of the analysis against an acceptability criterion or criteria. The third step is the focus of this paper where the novelty of this work appears. Rather than drawing a deterministic FTD for identifying probability of occurrences of the failure events a probabilistic one is suggested to cater for any risks or uncertainties involved in the system. By allowing probabilistic input of basic events a probabilistic top event is produced giving managers more freedom to check among a range of failure probabilities that the system might fall in rather than one limited deterministic failure value. This gives more practicality to the assessment of the whole system resulting in better actions and higher reliable performance.

1. Systems Failure and Their Causes

Failure of a system or a component in a system can be a catastrophic phenomenon which may result in severe physical and social consequences. Systems failure - either engineering systems, management systems or socio-technical ones or other sort of defined systems - can be caused by a vast number of factors which may interactively contribute towards the failure of a system’s performance as a whole. As Sauer [1] put it in his study for systems failures: "All kinds of technological and organisational systems suffer failure". Typically, each type of system experiences a different kind of failure within its own field. Sauer's statement can be seen to be valid when it comes to complex systems which is expected to work in complex interrelated subsystems. However, the major problem that faces systems engineers is the quantification of risk involved in the performance of the system with its different components. Obviously, this quantification will facilitate the prediction of the system success or its failure and malfunctioning. Thus, the problem of risk quantification should be fully recognised and thoroughly looked into to get
a realistic picture of the size of the failure problem. Additionally, in the author's personal opinion, there is a big drawback in the way systems engineers assess their system performance, mainly due to:

1. Only applying deterministic methods in their assessment without forecasting or understanding the stochastic nature of the factors influencing the system's internal and external performance.
2. Lack of establishment of a reliable and effective method by which they can monitor, audit and evaluate all component performance and predict the possibilities of failure in their functions before accepting the system for operation.

2. System Reliability Assessment

To avoid these drawbacks systems engineers need a method that can ensure the robustness and flexibility of their system to cope with any malfunctioning and uncertainties. They need to perform system reliability assessment to evaluate the performance of all the individual components of the system. Reliability analysis offers the solution. Furthermore, in order to understand the probabilistic nature of the system this paper suggests that systems engineers should not only apply qualitative reliability techniques in assessing the performance of their system but quantitative probabilistic risk methods must also be introduced [2] and [3]. Unfortunately, most studies done in reliability evaluation highlight and diagnose the problem in qualitative rather than quantitative terms [4]. Confirming the importance of introducing quantitative reliability methods Andrews and Moss [5] showed that reliability technology has benefited significantly from applying some qualitative and quantitative reliability techniques such as Fault Trees, Markov and human reliability analysis.

2.1 Terminology and Definition of Reliability

Aggarwal [6] quoted a detailed definition by the Electronics Industries Association (EIA) which defined reliability in general terms by stating that: "Reliability of an item (a component, a complex system, a computer program or a human-being) is defined as the probability of performing its purpose adequately for the period of time under the operating and environmental conditions encountered". Similar definitions of reliability can be found in articles written by a number of authors and reliability theorists such as [7], [8], [9], [10], [11], [12] and [13].

2.2 Objective of Probabilistic Analysis

Reliability theory is mainly concerned with the occurrence and non-occurrence of failure events. Probability theory, on the other hand, is used along with reliability theory to enable managers to determine the chances of occurrence of these uncertain events quantitatively. The objective of probabilistic analysis of systems is to assess the degree of guarantee, from a system performance perspective, which can be associated with a given system during its operation. Thus assessing the risks associated with system’s components is useful for improving their functions by minimising chances of their occurrence.
3. **Risk Assessment**

Before analysing systems reliability it is important to understand what is risk assessment. Risk assessment is widely recognised as a systematic process for quantitatively (or qualitatively) describing risk. Bedford and Cook [14] characterise risk with two particular elements: hazard (a source of danger) and uncertainty (quantified by probability). The total risk is the sum of the products of the consequences multiplied by their probabilities.

### 3.1 The Challenge: Realising the Problem

Expectations of reliability are increasing and the consequences of reducing systems failure have never been greater. Systems engineers are committed to supplying reliable systems with low risk associated with them. To maintain that commitment into the future, systems engineers must address an array of uncertainties. In this uncertain environment, the traditional methods of performing system reliability assessments are no longer adequate. The traditional tools use a deterministic approach to calculate the impact of potentially disruptive events, without regard to the probability of their occurrence. A probabilistic approach is therefore required for assessing the performance of the system with its components.

### 3.2 The Solution: Introducing the Probabilistic Risk Assessment

Assessing the reliability performance of complex system involves dealing with events whose occurrence cannot be predicted easily. Not only a good descriptive procedure of the system’s components is required but also the solution requires some means by which the likelihood of the events can be expressed in terms of quantitative methods. This places an emphasis on the importance of enhancing the reliability analysis with probabilistic risk analysis technique for evaluating system’s risk in terms of calculating its failure events and the corresponding range of probabilities values associated with those failures. This procedure of integration has been extensively and successfully used to evaluate complex systems under the name of Probabilistic Safety or Risk Analysis [PSA/PRA]. PRA is an approach developed over the last 20 years to estimate quantitatively the risks associated with complex engineering systems, such as nuclear power plants, chemical process facilities, waste products and space systems.

4. **The Probabilistic Risk Assessment (PRA) Approach**

#### 4.1 PRA Characteristics

PRA enables decision makers to balance reliability and risk. PRA provides a more accurate tool for assessing systems reliability. Unlike traditional deterministic contingency analysis tools, PRA calculates a measure of the probability of undesirable events and a measure of their severity or impact. In a PRA, risk is characterised by two quantities [15]:

1. The magnitude (severity) of the possible adverse consequence(s) (for example failure of a certain component or components in a mechanical
or electrical physical system, failure percentage of a department in a socio-technical system, etc.).

2. The likelihood (probability) of occurrence of each consequence. (i.e., the number of occurrences or the corresponding probability value to every departmental failure percentage, etc.).

PRA usually answers three basic questions [3]:

1. What can go wrong with the studied system, or what are the initiators or initiating events (undesirable starting events) that lead to adverse consequence(s)?
2. What and how severe are the potential detriments, or the adverse consequences that the system may be eventually subjected to as a result of the occurrence of the initiator?
3. How likely to occur are these undesirable consequences, or what are their probabilities or frequencies?

The answer to the first question is a set of failure scenarios. The second question requires the evaluation of the probabilities of these scenarios, while the third estimates their consequences. Two common methods of answering this last question are the Event Tree Analysis and Fault Tree Analysis [16], and [17]. The last one is the one this work will employ for illustrating the proposed PRA approach.

4.2 PRA Stages

In this work it is recommended to use quantitative risk and reliability techniques together with the qualitative ones for building a Probabilistic Risk Assessment (PRA) approach for assessing system reliability. The proposed PRA involves four main stages under two main risk headings:

1. **Risk estimation:** which encompasses a detailed description of the risks scenarios, this includes:
   1) Identification of the potential events and their modes of failures.
   2) The estimation of the consequences of these failures on the total system.

2. **Risk acceptability:** which involves determination of an acceptable level to the risk encountered and to ask how safe is safe enough? This includes:
   3) The estimation of the probability of occurrence of each event of failure.
   4) Comparison of the results of the analysis against acceptability criteria.

The first two stages of risk estimation are mainly performed using qualitative risk and reliability techniques like the Reliability Block Diagram (RBD) to represent the connections between system’s components and the Failure Mode and Effect Analysis (FMEA) to represent the knowledge about the system's performance in terms of identifying the potential failing events and their mode of failures in addition to their consequences on the total system function then preparing what is called Knowledge Base Production Rules (KBPR). These methods will be illustrated in the application example at the end of this paper. However, for more understanding of how they are prepared the reader can refer to references like: [5], [7], [9], [18], [19], and [20]. On the other hand, the third and fourth stages of risk acceptability use different quantitative techniques to provide the probabilistic assessment suggested in this work. For more details, see for example [2], [6], [8], [10] and [21].
The third stage is the main focus of this paper where it suggests transforming the qualitative Fault Tree Diagram (FTD) of the Fault Tree Analysis (FTA) to a quantitative one for identifying the probability of occurrences of the system’s failure events. This is done by entering the expected failure percentages (rates) of all the basic events and their corresponding probabilities values, then calculating the expected failure percentages and the corresponding probabilities values of all dependent (intermediate) events followed by the top undesired event as will be shown in the illustrative example next.

5. **Illustrating the PRA Approach in an Example**

5.1 **Systems Description**

To illustrate how the proposed PRA approach in this work can give insight into probabilistic evaluation and assessment of reliability to the system performance, the system under investigation is a physical system used to pass electric power to two terminals personal computers as shown in Figure 1. The system is composed of a Source (S) motor power which is connected in series to a Circuit Breaker (CB). Both are connected in series to two groups of couple Transformers (TR1 and TR2) and couple of personal computer terminals (PC1 and PC2) where each group of transformers is connected in series to one personal computer terminal. Both joined groups are joined in parallel connection. The source of this example is obtained from literature on reliability evaluation [9]. Similar types of systems can be found in [12] but representing electric bulbs instead of computer terminals.

![Diagram](source: Pages and Gondran, 1986 [9])

5.2 **System Reliability Assessment: The PRA Approach**

**Main assumption:** In this computer system, it is assumed that in real application any of the components of the system can be defective at any time during its operation and that systems engineers cannot wait until they monitor the failure of each component in application then record them for future remedy actions. Hence a formal reliability evaluation to predict potential modes of failures, their possible causes and their effects on the total system performance has to be conducted. Furthermore, systems engineers have to define the possible failure scenarios of the system and to predict beforehand, either from previous experience (if it is an existing system) or by guess (if it is a new system), the expected failure percentage of every basic event that can happen and the likelihood (probability) of its occurrence. To show how this reliability evaluation can be performed, the author has developed a DSS programme called ManageRely (Management Reliability) to illustrate the steps of this PRA approach. The application was initially designed to assess
the reliability of a socio-technical system of organisations in the construction industry. However, the same programme is used, in this work, to illustrate the PRA procedure to assess the reliability of this physical computer system.

It is worth mentioning here that a short overview was done on available PRA software in the market. There are many Probabilistic Safety Assessment (PSA) software packages out there, but there is only one for the serious PSA professional: RISKMAN. It incorporates the four major steps of PSA analysis into one package: data analysis, system analysis, natural hazard analysis and event tree analysis. It makes use of modern mathematical techniques for avoiding approximations. However, when approximations must be done, the exact value of the error is calculated which can help in reducing the guessing of how accurate your results are. SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations) is another probabilistic risk and reliability assessment software tool developed for the U.S. nuclear regulatory commission (NRC) by the Idaho National Laboratory. SAPHIRE gives a user the ability to create and analyze fault trees and event trees using a personal computer. In terms of reliability evaluation fault trees can be constructed and analysed to obtain different measure of system unreliability, event importance measures, include: Fussell-Vesely; Birnbaum; risk increase ratio and interval; risk reduction ratio and interval; group; and uncertainty importance. Another risk analysis software is RiskSpectrum®; Risk Management Software which is a product of the most advanced Risk and Reliability Analysis software in the world. The software includes advanced tools for fault tree and event tree analysis, documentation, risk monitoring and failure mode and effect analysis. All these packages do not use the 2nd-order assessments as recommended by ManagerRely. Although more work required to make ManageRely a commercial package, it is sought here that it is still useful in analysing and assessing the probability of failure of systems, especially those of management systems that does not need high mathematical accuracy as mechanical and electrical systems. It can give systems management a sense of the ranges the failure of their departments can fall within. This is done using a two dimensional probabilistic approach rather than one dimensional deterministic value.

Figure 2: RBD for the Computer System Model (as Appears in ManageRely Programme)
5.3 Steps of the PRA Methodology

The first step in the PRA process starts with the systems engineers performing a thoroughly systems approach study where the main mission, goals and objectives of the system and its components are identified and defined. Then, for reliability evaluation, the system is displayed and modelled on a chart called Reliability Block Diagram (RBD) showing series, parallel or series-parallel relationships between its various components, as in Figure 2.

The second step is to perform PRA as follows:

A] Applying Qualitative Reliability Techniques: This is done by using:
  1) The Failure Mode and Effect Analysis [FMEA]: where a detailed study is performed to identify the modes of failure expected in the system and to determine their possible causes of failure with their effect on the total system. Figure 3 illustrates the FMEA table as represented in ManageRely for the whole system. This is followed by applying a qualitative representation called:

```
Figure 3: FMEA of The Whole System
(as Appears in ManageRely Programme)
```

  2) The Knowledge Based Production Rules [KBPR]: as in Figure 4 which aims to represent the knowledge about the system in a comprehensive manner using 'If..then" failure scenario. This important technique then facilitates the application of:

```
Figure 4: KBPRs For The Computer System
(as Appears in ManageRely Programme)
```

  3) The Fault Tree Analysis [FTA]: where the qualitative Fault Tree Diagram [qual_FTD] is constructed as shown in Figure 5 where its branches demonstrate the KBPR table. FTA has the advantage of identifying the weak components of the system on the screen of the computer to assist managers to assess their performance and allow to make necessary actions for
improving their performance. In this qualitative FTD, as shown in Figure 5, the Top Event TE (failure supply to the PC1 and PC2, which means the failure of the whole system to operate) is the system's undesired event under analysis. It is produced from the occurrence of two Intermediate Events: IE1 (failure supply to PC1) and IE2 (failure supply to PC2) connected by an "AND" gate showing that both of them have to occur in order that the top event occurs. Event IE1 is produced from Basic Event; BE1 (primary failure of Transformers TR1) and two intermediate events; IE1-1 (complete failure of Source component S) and IE1-2 (complete failure of Circuit Breaker component CB) which are all connected by an 'OR' gate showing that only one of them has to occur in order that IE1 occurs. Similarly, event IE2 is produced from BE6 (primary failure of Transformers TR2) and intermediate events IE1-1 and IE1-2 represented by two triangle transfer gates 1 and 2. Event IE1-1 is produced from basic events BE2 (primary failure of the S component) and BE3 (primary failure of supply line to the S component). While IE1-2 is produced from basic events BE4 (primary failure of supply line to the CB) and BE5 (fire in the equipment room of the CB).

**B) Applying Quantitative Reliability and Risk Techniques**

As stressed in this work, qualitative reliability techniques are not enough to achieve reliable results. The results of the qualitative analysis are only descriptive which cannot give any feeling of the dangers encountered in the performance of the system. Hence, a thorough quantitative analysis should be conducted to enhance the previous qualitative reliability techniques with some useful quantitative ones. Hence, a quantified evaluation is done for the qualitative FTD. The designed programme offers friendly interactive screens for producing the probability curves in a relative frequency form as well as in cumulative form. This is the quantitative Fault Tree Diagram [quant_FTD].

---

**Figure 5: Qualitative FTD Of The Computer System**  
(as Appears in ManageRely Programme)

**Failure Values and Probability Inputs / Calculations:**

a) **Deterministic Type of Failure Values:** in this option it is assumed that systems engineers are confident (i.e. certain) about the percentage failure value (events performance level) that is likely to happen for each basic event.
Users are offered the freedom to input the deterministic value of failure percentage on the horizontal scale from 0% to 100% as shown on the graph in the top right corner of the screen in Figure 6 where the input for basic event BE1 is illustrated. Because this is a certain value its chance of occurrence is also certain i.e. automatically the probability of any percentage value of failure chosen is equal to 1.0.

b) Stochastic Types of Failure Values: These are either objective or subjective types of probabilities of failures:

1) Objective Probability Type: In this type of probability it is assumed that the user has previous knowledge about the performance of the component, for example, from previous experience or previous records, hence s/he can input the percentage values of failures that are expected to happen and their likely chances of occurrences.

Figures 6 shows the objective failure percentage inputs and calculations of the probabilities of the basic event BE1 (primary failure of TR1) on the FTD. The graph produces the relative frequency curve from which automatically the cumulative probability curve is obtained as shown in Figure 6.

2) Subjective Probability Type: Figures 8 shows the different procedures used for inputting and calculating the subjective probability curves of the basic events. In this method ManageRely offers two techniques. These are: (1) The Fractile method (The Interview method) and (2) The Utility method (The Lottery method) [22]. In both techniques, the probability curve is first plotted in a cumulative form from which the relative frequency curve is deduced then every basic event expected failure percentage and its corresponding probability value are calculated. In Figure 8 the Fractile method is used to produce the probability curve of basic event BE2 while the Utility method is used to determine the curve of basic event BE6. The other basic events BE3, BE4 and BE5 were obtained using the direct objective probability inputs.

The third step in this PRA approach is to calculate the probability values of the dependent events (intermediate events and top event) as shown in Figure 8. As in normal FTA calculations, this is done by using the laws of addition (for OR gates events) and multiplication (for AND gates events) of the expected failure percentage values and the corresponding probability values of all basic...
events. This produces the probabilistic values of the intermediate events and the top undesired event.

In this part, it is worth noting here that there is a debate on how meaningful 2nd-order probabilities can be assigned, in particular as 1st-order probabilities are recognized to be problematic. Due to limited space and as this is not within the scope of this paper to explain the different methods for explaining this problem, however a number of literatures like [22] and [23] explains some methods to solve this problem as well as other literature reviewed the means and methods on determining assessing risks with evaluating second order probability [23], the uncertainty in PRA [24] and eliciting probabilities from Experts [25].

6. Interpretation of the Results

6.1 Interpretation of Results From The Deterministic Approach

To reveal the difference between the deterministic risk approach and the probabilistic risk approach as proposed in this work, a deterministic FTA is performed with all basic events entered as deterministic (i.e. certain) one failure percentage value with a probability value of 1.0 as shown in Figure 7. Accordingly, the top event gave a value of failure = 92.82% with certainty (i.e. \( P(92.82\%) = 1.0 \)). By inspecting the tree it would be noticed that this high value was obtained from multiplying (AND gate) the failures of IE1 \( P(95.11\%) = 1.0 \) and IE2 \( P(97.59\%) = 1.0 \). Obviously IE2 (failure of Supply PC2) contributed more to the top event failure value. Therefore by tracing the tree back to investigate why IE2 is so high, it would be found that it came from the addition rule (OR gate) of IE1-1 (68.05%) and IE1-2 (69.55%) and BE6 (69.86%). Since IE1-1 (failure of S) and IE1-2 (failure of CB) are common in both branches of the tree as represented by the transfer triangle gates 1 and 2 on the tree, therefore the cause of this high value is due to BE6 (primary failure of TR2). Systems engineers should now find why the group of Transformers TR2 is not performing as expected since it is contributing with a high value to the failure of the whole system.

![Figure 7: Inputs and Calculations Of The Failure Events On The FTD--[Deterministic Approach] [ManageRely Screen Dump]](image)
6.2 Interpretation of Results From The Probabilistic Approach

As claimed in this work, the deterministic approach is not reliable to make a good understanding of the system performance as the failures of the basic events are obtained with certainty and this limits the thinking of systems engineers to accepting one output value of failure of the dependent events and the top event which does not reflect a realistic view about the system operation in real life application and may result in wrong management actions. Therefore, it is believed that the probabilistic FTD as in Figure 8 gives more realistic and reliable idea about the system performance. By inspecting the probabilistic FTD where the basic events are entered in a probabilistic fashion as described in the previous section, it was found that the top event's expected failure gave a failure value of 40.49% with probability of 0.664 i.e. P(40.49%) = 0.664 not with certainty as in the deterministic interpretation producing an overall risk value of 26.885 [i.e. 40.49 (consequence) x 0.664 (probability)]. By continue inspecting the tree it would be noticed that this value was obtained from multiplying the failures of IE1 [P(64.14%) = 0.81] and IE2 [P(63.12%) = 0.82]. Obviously IE1 (failure of Supply PC1) with risk value of 51.953 is higher than IE2 with risk value of 51.758. Hence IE1 contributed more to the top event failure value. Also by tracing down the tree to investigate why IE1 is so high, it would be found that it came from the addition rule of IE1-1 [P(14.57%) = 0.15] with risk value of 2.1855 and IE1-2 [P(40.00%) = 0.68] with risk value of 27.20 and BE1 [P(29.75%) = 0.42] with risk value of 12.60. Since IE1-1 (failure of S) and IE1-2 (failure of CB) are common in both branches of the tree as represented by the transfer triangle gates 1 and 2 on the tree, therefore the cause of IE1 value is due to BE1 (primary failure of Transformer TR1) which is higher than BE6 [P(28.05%) = 0.34] with risk value of 9.537. This means that chances of causing the overall probability of failure of the whole system (i.e. the top event) with a risk value of 26.885 is contributed to the malfunctioning of Transformers TR1 not Transformers TR2 as given by the deterministic approach. This is an important finding that systems engineers have to take care of when choosing risk approaches for assessing systems’ reliability.

Figure 8: Inputs and Calculations Of The Failure Events On The FTD--[Probabilistic Approach] [ManageRely Screen Dump]
7. Conclusions

In the reliability context, assessing the reliability performance of complex systems involves dealing with events whose occurrences are sometimes not easily predicted. Handling such events which are not deterministic (i.e. stochastic or uncertain) is thus an important issue facing systems designers. This paper focuses on the importance and effectiveness of assessing the reliability of the overall system performance by offering a probabilistic risk assessment (PRA) approach for assessing its individual components and to help them to analyse and thoroughly understand the behaviour of the system realistically and ensure its success and survival in long-term applications.

By inspecting and comparing between the deterministic and the proposed PRA approach this study revealed the benefit of quantifying the FTD as it helped in pointing out the defective components which need to be checked, monitored or replaced for more reliable performance of the whole system. Similarly systems engineers can track the probabilistic FTD to identify other defective components in the system for taking proper remedial actions to improve the whole system reliability. Additionally, if systems engineers for example, set an acceptability criteria value of expected failure percentage of 50% or less with corresponding probability value of 75% to consider the system performance satisfactory, i.e. P(System Failure % <= 50%) = 0.75, then by inspecting the deterministic approach the result of the top event (representing system failure) is P(92.82%) = 1.0 which in most cases will not satisfy this requirement as the resulting probability will always be 1.0 while the more realistic probabilistic approach satisfies this requirement where P(40.49%) = 0.664. It is thus believed that this PRA approach is more realistic to apply than the deterministic one as it proves impractical to accept one certain (deterministic) value of failure by which the component(s) could fail. By allowing probabilistic input of basic events a probabilistic top event is produced giving managers more freedom to check among a range of failure probabilities that the system might fall in rather than one limited deterministic failure value. This gives more practicality to the assessment of the whole system resulting in better actions and higher reliable system performance.

References