Reliability Engineering and System Safety **21** (1988) 215–223

Some Considerations on Reliability Theory and Its Applications

Terje Aven

Rogaland University Center/Rogaland Research Institute, Box 2557, Ullandhaug, 4001 Stavanger, Norway

(Received 16 October 1987)

ABSTRACT

In this paper we discuss some main topics within reliability theory and its applications. These include for example, modelling of systems of dependent components, identification of critical components, modelling of repairable systems, and the use of multistate models.

The starting point for the discussion is Bergman's review paper on reliability theory and its application (Scand. J. Statist., ***12*** *(1985) pp. 1–41).*

1 INTRODUCTION

Today there exists a considerable published literature on reliability theory and its applications. Most of this literature is on pure reliability theory. Little attention has so far been devoted to the problem of practical implementation of methods and techniques developed. This has resulted in a huge gap between the theory and the applications of the theory.

This paper discusses some aspects of vital importance when reliability theory is applied to real-life problems. The starting point for the discussion is Bergman's review paper on reliability theory and its application.[1]

We will use standard nomenclature from reliability theory without further comments. When writing 'reliability' we mean either reliability or availability, depending on the situation considered.

Reliability Engineering and System Safety 0951-8320/88/$03·50

2 RELIABILITY THEORY AND ITS APPLICATIONS

When performing a reliability analysis, the analyst must come to a decision on a number of questions such as:

1. Are the components (basic events) to be considered as stochastically independent?
2. Is a binary representation of the system and components sufficient or is it necessary to use a multistate representation?
3. Are the components/system to be considered as repairable or non-repairable? Can steady-state probabilities be justified?
4. How is the uncertainty of component reliabilities to be handled?
5. How are the most critical components (subsystems) to be identified?
6. Which calculation methods/algorithms are to be used?

Below some general considerations on these topics are given.

2.1 Independent components

In most reliability analyses the components of the system are assumed stochastically independent. In practice, however, there are often dependencies between components due to for example common mode failures. This type of failure involves the simultaneous outage of two or more components owing to a common cause. One of the most important steps in a reliability analysis is to identify and separate out common factors in such a way that the components can be regarded independent (cf. Ref. 1, p. 3). Such a separation process can be difficult to carry out, but it is usually necessary in order to correctly quantify the system reliability. To achieve the

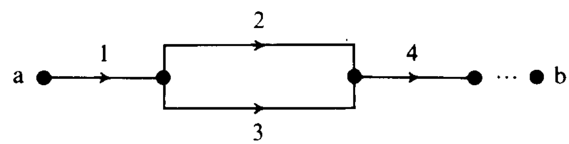

Fig. 1. An example of a flow network.

independence, multistate components must in some cases be introduced. Consider as an example the flow network in Fig. 1. The state of the system equals the maximum flow that can be transmitted through the network from a to b. Suppose the components 2 and 3 are either functioning or not, and the possible flow capacities for component 2 are 0 and 10, and for component 3, 0 and 20. Suppose also that there is some sort of dependency between these two components. Now, by considering the components 2 and 3 as one component, we can remove the dependency from the top-level analysis. This new component has possible flow level capacities 0, 10, 20 and 30. Of course, in order to calculate the probability distribution of the random capacity of this new component or to simulate the capacity process, we must take into account the dependency between the two components 2 and 3. But this is a problem at a lower system level and special techniques such as Markov-analysis can be used.

Another approach for taking into account dependency is to obtain bounds on the system reliability, assuming that the components are *associated* and not necessarily independent. As far as applications are concerned, this approach does not seem to have won through. The main reason for this is the fact that this method usually leads to very wide intervals for the reliability (cf. Rausand's contribution in Ref. 1). If the problem is to compare different design alternatives or system modifications, or identify the most critical components, such intervals are very little informative and represent a poor basis for making decisions.

Bent Natvig states in his contribution in Ref. 1 that wide intervals 'just reflects the fact that precise statements in reliability are impossible when just having vague information on the dependencies coming into play, as is very usual in a risk analysis of a real-life system'. As a reply to this it can be said that in a *first phase* of a reliability or risk analysis, the information about the dependency might be so vague that we are forced to apply bounds based on associated components. However, in order to arrive at results that can be used as a basis for making decisions, the dependencies must be looked more closely into and separated out from the top-level analysis.

2.2 Binary/multistate representation

The traditional reliability theory based on a binary approach has recently been generalized by allowing components and systems to have an arbitrary finite number of states.

For most reliability applications, binary modelling should be sufficiently accurate, but for certain types of applications such as gas/oil production and transportation systems, a multistate approach is usually required for the system and some components.

In a gas transportation system, for example, the state of the system is defined as the rate of delivered gas, and in most cases a binary model (100%, 0%) would be a poor representation of the system. A component in such a system may represent a compressor station comprising a certain number (M) of compressor units in parallel. The states of the component equal the capacity levels corresponding to M compressor units running, $M-1$ compressor units running, and so on.

For highly available systems, which is the most common situation in practice, multistate components can often be considered as binary components without any significant loss of accuracy. For example the compressor station mentioned above may be represented by two states: M compressor units operating and $M-1$ compressor units operating. The possibility of two or more units being out of operation at the same time are then ignored.

Much research has recently been carried out on flow network systems such as gas/oil production and transportation systems and power transmission systems, see e.g. Refs 2 to 5. Undoubtedly this type of system is one of the best examples of the usefulness of multistate modelling.

2.3 Repairable/non-repairable units

Most real-life systems are repaired at failures rather than being replaced (the concept 'system' might here refer to a component). Nevertheless, repairable systems have received very little attention in reliability papers and texts. If a repairable system is analyzed, it is usually assumed that the failure process can be described by a renewal process, i.e. the system is good as new after a repair. Once this assumption has been made, the chronological order in which the interarrival times to failure occur is unessential, so the interarrival times can in fact be treated as originating from non-repairable systems. But it is obvious that the chronological order might be an extremely important aspect of a repairable system failure data set. For example, the chronological data might indicate that the system has an improving (deteriorating) reliability.

To model repairable systems, a point process approach should be adopted. For systems where the 'good as new' assumption is unrealistic, the nonhomogeneous Poisson process (NHPP) is usually the most appropriate model. The NHPP is thoroughly studied in the literature, see e.g. Refs 6–10.

Asher and Feingold have in a number of papers discussed various aspects of repairable systems reliability. Their work has contributed very much to the clarification of concepts and identification of relevant methods. Their book[7] is strongly recommended.

If a renewal process or more generally a semi-Markov process can be justified, the limiting or long run availability of the system can in most cases easily be determined. For evaluating the availability of a system consisting of a number of components, it is usually assumed that the component availability is equal to this limiting availability. Such an assumption represents in most situations a good approximation. In applications there is seldom enough information available to determine the system availability as a function of time.

2.4 Uncertainty of component reliabilities

Lack of relevant component reliability data is a problem in many reliability analyses, in particular, when the purpose of the analyses is reliability *prediction*. However, reliability analysis is primarily a tool for making decisions, for example related to choosing one out of a number of possible design alternatives, or to identify components/subsystems which are natural candidates for reliability improvement. The system reliability is a factor that has to be evaluated when such decisions are to be taken whether the uncertainties are large or small. Therefore, the aim must be to provide the best reliability data (including expert opinion) that are available, and possibly perform sensitivity analyses with respect to the data that are most uncertain.

When for example comparing various design alternatives, it is the differences in system reliability level that is of interest. The uncertainties related to these differences are in general much lower than for the absolute reliability values.

2.5 Identification of critical components (subsystems)

The purpose of many reliability analyses is to identify weaknesses in a design or to identify components (subsystems) on where to allocate efforts on reliability improvements, and for that purpose some sort of criticality measure must be defined.

A number of measures have been proposed, see for example Refs 1, 3, 5 and 11–13; see also Ref. 14. As mentioned by Bergman,[1] 'for the choice of a specific measure it is important to make clear in what sort of situation it is to be used. Undoubtedly, different situations call for different measures'.

Our experience is that the following measure is appropriate in a large number of situations, in particular during design:

$$\text{The importance of component } i \text{ (subsystem } i) = A_i - A \overset{\text{def}}{=} I_i$$

where A is the reliability of the system, and A_i is the reliability assuming that component i is in the best state. Thus the importance of component i expresses the system reliability improvement *potential* of the component, in other words I_i expresses the unreliability that is caused by imperfect performance of component i. This measure can be used for all types of reliability definitions, and it can be used for repairable or non-repairable systems. Many of the existing measures apply only to non-repairable systems. This makes the application of these measures quite limited since most real-life systems are repairable.

It should be noted that for a highly reliable coherent system with reliability interpreted as the probability that the sytem is functioning at a certain point in time, the measure I_i is equivalent to the well-known Vesely–Fussells importance measure.[15] In fact, in this case

$I_i \approx$ sum of the unreliabilities of the minimal cut sets which include component i.

The measure I_i gives like the Vesely–Fussells measure the same importance to all the components of a parallel system, irrespective of component reliabilities. This is as it should be because each one of the components has the *potential* of making system unreliability negligible, for example by introducing redundancy. But as pointed out above, the appropriateness of the measure depends on what kind of characteristics we want the measure to reflect. In the design phase the system reliability improvement potential (I_i) might be the most informative measure, but for a system with frozen design, the Birnbaum[16] measure might be more informative since this measure reflects how small component reliability improvements effect system reliability.

Some importance measures are time dependent, for example Birnbaum's measure, Vesely–Fussells measure, and the above measure I_i for certain definitions of reliability. For repairable systems, however, limiting component availabilities are usually adopted, so the time dependence is in fact eliminated.

2.6 Methods/algorithms for reliability evaluation

The reliability of a coherent system is usually found using a two step procedure:

1. Identification of the minimal cut sets of the fault-tree/network.
2. Computation of the reliability by using the inclusion–exclusion method, or another evaluation method based on minimal cut sets.

For highly reliable systems, the most common situation in real-life, the first upper bound on the unreliability using the inclusion–exclusion method, i.e. the sum of the unreliabilities of the minimal cut sets, is an excellent approximation. In general, the algorithms by Abraham[17] and Aven[18,19] can be used for exact calculation of the reliability based on the minimal cut sets, see also Ref. 20.

The above procedure can be carried out in practice because relevant computer codes are available, see Refs 11, 18, 19 and 21–26.

The number of minimal cut sets for complex systems might be extremely large. However, by using modular decompositions it is often possible to reduce the number of minimal cut sets significantly and simplify the calculations. The strategy is then to find the minimal cut sets for each module and compute the corresponding reliability. The reliability of the whole system is found by inserting the module reliabilities into the reliabilities for the organizing structure.

If the number of minimal cut sets is very large, some kind of cut-off procedure might be required, for example the neglection of minimal cut sets of a high order. An upper bound on the error in the result due to the cut-off should then be established, cf. e.g. Refs 24 and 27.

The minimal cut sets also gives a useful qualitative description of the system since they constitute the possible minimal combinations of component failures which imply system failure. The minimal cut sets are also needed in order to obtain bounds on system reliability for associated components, and in order to compute certain reliability importance measures, see e.g. Refs. 3, 11, 28 and 29.

If the problem is just to compute system (un)reliability, then we can alternatively use a direct approach which is not based on minimal cut sets, see e.g. Ref. 30.

The *factoring algorithm* (see e.g. Ref. 1) is very often referenced as an efficient algorithm for *exact* reliability computations. For hand-calculations of small networks this algorithm is undoubtedly appropriate. However, there does not *yet* seem to exist any efficient computerized version of the algorithm, and without such a computerized version the usefulness of the algorithm is rather limited from a practical point of view.

For reliability evaluations of flow network systems, the approximation-formulae stated in Refs 3 and 4 are usually appropriate. For exact calculations the algorithm by Doulliez and Jamoulle[31] is very efficient. This algorithm does not require that the minimal cut sets for the actual flow level are known. If these are identified, the algorithm by Aven[18] can be used to calculate the reliability.

Formulae (bounds) for the average unavailability/mean fractional dead time of a coherent system with periodically tested components are given in Ref. 32.

For some Monte Carlo simulation programs for reliability evaluations, see e.g. Refs 3, 11 and 26. A discussion of the advantages and disadvantages of the simulation approach compared to an analytical approach is given in Ref. 3.

REFERENCES

1. Bergman, B., On reliability theory and its applications with discussion, *Scand. J. Statist.*, **12** (1985), pp. 1–41.

2. Rueger, W. J., Reliability analysis of networks with capacity-constraints and failures at branches and nodes, *IEEE Trans. Reliability*, **35** (1986), pp. 523–8.
3. Aven, T., Availability evaluation of oil/gas production and transportation systems, *Reliability Engineering*, **18** (1987), pp. 35–44.
4. Aven, T., Availability evaluation of flow network systems, Report Rogaland University Center/Rogaland Research Institute, Stavanger, Norway, 1987.
5. Aven, T. and Østebø, R., Two new component importance measures for a flow network system, *Reliability Engineering*, **14** (1986), pp. 75–80.
6. Crow, L. T., Reliability analysis for complex repairable systems, in *Reliability and Biometry*, F. Proshan and R. J. Serfling (eds), Society of Industrial Applications of Mathematics, 1974, pp. 379–410.
7. Asher, H. E. and Feingold, H., *Repairable System Reliability: Modelling, Inference, Misconceptions and Their Causes*, Marcel Dekker, New York, 1983.
8. Aven, T., Determination/estimation of an optimal replacement interval under minimal repair. *Optimization*, **16** (1985), pp. 743–54.
9. Aven, T., Estimation and testing in counting processes having linear intensity form, with applications to analysis of failure time data, Report Rogaland University Center, Stavanger, Norway, 1987.
10. Aven, T., Some tests for comparing reliability growth/deterioration rates of repairable systems, Report Rogaland University Center/Rogaland Research Institute, Stavanger, Norway, 1987.
11. Henley, E. J. and Kumamoto, M., *Reliability Engineering and Risk Assessment*, Prentice-Hall, Englewood Cliffs, NJ, 1981.
12. Natvig, B., A suggestion of a new measure of importance of system components. *Stochastic Proc. Appl.*, **9** (1979), pp. 319–30.
13. Natvig, B., New light on measures of importance of system components, *Scand. J. Statist.*, **12** (1985), pp. 43–54.
14. Aven, T., On the computation of certain measures of importance of system components, *Microelectronics and Reliability*, **26** (1986), pp. 279–81.
15. Fussell, J. B., How to handcalculate system reliability and safety characteristics, *IEEE Trans. Reliability*, **24** (1975), pp. 169–74.
16. Birnbaum, Z. W., On the importance of different components in a multicomponent system, in *Multivariate analysis—II*, P. R. Krishnaiah (ed.), Academic Press, New York, 1969, pp. 581–92.
17. Abraham, J. A., An improved algorithm for network reliability, *IEEE Trans. Reliability*, **20** (1979), pp. 58–61.
18. Aven, T., Reliability evaluation of multistate systems with multistate components, *IEEE Trans. Reliability*, **R-34** (1985), pp. 473–9.
19. Aven, T., Reliability/availability evaluation of coherent systems based on minimal cut sets, *Reliability Engineering*, **13** (1986), pp. 93–104.
20. Locks, M. O., Recursive disjoint products, inclusion–exclusion. and min-cut approximations, *IEEE Trans. Reliability*, **29** (1980), pp. 368–71.
21. Fussell, J. B., Henry, E. B. and Marshall, N. M., MOCUS—a computer program to obtain minimal cut sets from fault trees, Aerojet—Nuclear Comp.—1156, Idaho Falls, ID, 1974.
22. Willie, R., *Computer-aided Fault Tree Analysis, ORC 78–14*, Operations Research Center, University of California, Berkeley, CA, 1978.
23. Abel, U. and Bicker, R., Determination of all minimal cut-sets between a vertex pair in an undirected graph, *IEEE Trans. Reliability*, **31** (1982), 167–71.

24. Hoertner, H., Developments in system reliability analysis, *Nuclear Engineering and Design*, **71** (1982), pp. 337–9.
25. Pullen, R. A., AFTP fault tree analysis program, *IEEE Trans. Reliability*, **33** (1984), p. 171.
26. Lee, W. S., Grosh, D. L., Tillman, F. A. and Lie, C. H., Fault tree analysis, methods, and applications—a review, *IEEE Trans. Reliability*, **34** (1985), pp. 194–203.
27. Hughes, R. P., Fault tree truncation error bounds, *Reliability Engineering*, **17** (1987), pp. 37–46.
28. Barlow, R. E. and Proshan, F., *Statistical Theory of Reliability and Life Testing, Probability Models*. Holt, Rinehart and Winston, New York, 1975.
29. Funnemark, E. and Natvig, B., Bounds for the availabilities in a fixed time interval for multistate monotone systems, *Adv. Appl. Prob.*, **17** (1985), pp. 638–65.
30. Page, L. B. and Perry, J. E., An algorithm for exact fault-tree probabilities without cut sets, *IEEE Trans. Reliability*, **35** (1986), pp. 544–58.
31. Doulliez, P. and Jamoulle, J., Transportation networks with random arc capacities, *RAIRO, Recherche Operationelle Operations Research*, **3** (1972), pp. 45–60.
32. Aven, T., Formulae for the average unavailability (MFDT) of a coherent system with periodically tested components, *Microelectronics and Reliability*, **26** (1986), pp. 283–8.