A CONCEPT FOR THE SYSTEMATIC VERIFICATION OF A FAULT TREE ANALYSIS

K. Götz

Technischer Überwachungsverein Bayern Sachsen, München, Germany

Abstract

Safety systems and components, especially in nuclear power plants, are very complex and require a high reliability. The most common tool to define the reliability is the fault tree analysis. A systematic review is necessary to verify the correctness of these complex analyses. The aim of this work is to formulate requirements for a review from the standpoint of an independent expert.

1 Introduction

Safety systems, especially in nuclear power plants, consist of a high number of complex and difficult components. The consequences of a failure of one component are not easily to find out. The reliability of these systems is mainly calculated by fault trees. Additionally the evaluation of the fault trees enables statements about the reliability of the systems and the importance of components of the systems. For the verification of complex fault trees a systematic review is indispensable.

2 Elements of the systematic review

In general the review of a fault tree calculation includes the following topics:

- documentation of the state of the plant to be examined
- modelling of the boundary conditions of the systems
- structure of the fault trees
- input data of the calculation
- evaluation of the results of the analysis
For the investigation of these topics we recommend the following procedure:

- check of the fundamentals
- check of the system analysis and realization in the fault trees
- evaluation of the results
- variation of parameters and methods
- comparison with other analyses

3 Check of the fundamentals

The fundamentals of a fault tree analysis are the input data, the correct use of the program and the documentation.

To review the input data for a Probabilistic Safety Analysis (PSA), these data must be checked whether they represent the actual status of the system. If necessary the verification must be done by on site inspections. Especially older documents of plant design often do not represent the actual status. Calculations from the construction time of a plant possibly do not agree with the state of the art and new calculations are required.

Actual and planned measurements to change over parts of systems or complete systems must be mentioned if they are considered within a PSA. In general, all sources for the input data, the supporting documents, must be completely listed and verified.

Moreover the qualification of the used computer software, the correct use and documentation of the results must be checked.

The qualification of the software is sometimes a problem because there are no general qualification criteria and therefore individual qualification methods have to be developed.

Possible criteria to check the correct use of the software and the correct documentation are:

- all options of the software which enforce a systematic modelling, e.g. data bank options for identical components or groups of components and specifications of components (attributes) that allow different kinds of evaluation criteria must be used. There may not be mistakes in modelling and evaluating the fault trees, e.g. wrong connections of fault trees, wrong combinations of components and reliability data.

- the identity of the documented results and the input data must be traceable; different evaluations of a fault tree may cause different runs with changes in the data base (e.g. calculation with and without common cause failures). The documentation of these variation must include the data base, the fault tree input and the results.
4 Check of the system analysis and realization in the fault trees

The system analysis and the modelling of a fault tree is the main part of an analysis and therefore the main part of the verification, too.

4.1 Check of the system analysis and system boundaries

The **system description** must contain the system logic of the built fault trees. The main points of the verification (besides actuality and completeness) are:

- requirements to the complete system and parts of the system
- logic of the systems, way of working, separation of redundant systems
- boundary conditions, construction and requirements of the components

The **system data** analysis must include the variation of system tasks, branches and connections to and from other systems and concepts of repair and inspection.

The **operating data** section of the system analysis must give information about times of mission of the system and the concerned components, cases of requirements to the systems and necessary times and intervals for inspections and reparations of systems and components.

The **function criteria** of a system must include information about the degree of redundancy of systems, the efficiency of systems, the technical function criteria and the boundary conditions for the systems and components.

4.2 Check of the top events of the analysis

The top event of the fault tree defines the aim of the analysis. Therefore the definition of the top event must be exact. To check the top events, we recommend the following criteria:

- the aim of a fault tree analysis must be fixed definitely
- boundary conditions, that may influence the modelling of the systems must be exactly defined and documented
- if the fault tree analysis is the base of an event tree analysis, the boundary conditions and intersection points of both parts must be identical

Principally, as mentioned in the german psa-guide /2/, the boundary conditions of an analysis must be defined exactly, but not too limiting. Especially the influences of external and internal events, human reliability and accident management must be mentioned.
4.3 Verification of the base events

The failure mechanisms are fixed as base events in the fault tree. To check the used base events we suggest three criteria:

- the **description and delimitation** of the components are the base of the modelling of the fault tree and the assignment of reliability data from other sources. Reliability data can only be transferred if the components are similar, and have the same delimitation to energy supply and control systems. Therefore an exact delimitation is necessary.
- the **failure mechanisms** of the components are checked with the german "Ausfalleffektanalyse" /4/ or the "failure mode and effective analysis" (FMEA) from NUREG/NRC /3/. Both methods are useful for an effective and systematic search for possible failure mechanisms and failure effects. We recommend a check of the completeness and relevance of the used base events by the results of these analyses.
- the **requirements to reliability data** are very complex and cannot be completely discussed in this short paper, especially the way of detecting and treating common cause failures. So we just mention a few main requirements:

  - plant specific data; the sources of the data base and the way of developing the reliability data must be documented (mathematical method) and traceable
  
  - generic data; if generic data are used, the evidence of acceptability must be proofed; this acceptability of data depends on the type of construction, the energy supply, the control system, the delimitation and other component specific facts. The correct transformation of generic data to a fault tree analysis must be traceable.

  - plant specific and generic data; if there are plant specific data, but not enough to develop an acceptable statistic data base, the reliability data for a component must be a mixture of generic and plant specific data. We additionally have to check the way of mixing this data. The method must be correct (e.g. Bayesian Method /1/), documented and applicable.

4.4 Structure and completeness of the fault trees

Developing and examining the concept of the fault tree structure, the following points must be regarded /1/:

- handling of the analysis by several people
- easy handling and manipulating of parts of the fault trees
- connecting of different modules of fault trees
- traceability after a long period (important for living psa)
- traceability and examination by independent experts
Possible criteria to check the fulfilment of these requirements are:

- all facts of system design and boundary conditions (the results of the system analysis) must be reproduced within the fault trees. Only the documented technical facts may be regarded. The MCS-analysis must reproduce the system parts, components and failure modes of a system or a component and the results must agree with the cut-sets based on engineering judgement.

- the basic pattern of the fault trees, the logic division in subsystems and modules must be visible and the manipulation of the modules must be able with less effort of time and technical resources. The step by step development of the fault tree must follow the hierarchic structure of the systems. The names of the single fault trees have to support systematic work and traceability. There must be a systematic use of transfers and connections of fault tree parts and independent fault trees.

- the linkage of fault tree modules and the gates must be exactly described. This description must include the "what happens" at "which conditions".

- to support a systematic work and a "living psa" the available options of the computer program, mostly data bank options, should be used systematically. Additionally the options of the software must be used as far as possible to guarantee a flexibility in considering different requirements on the analysed systems (e.g. fire and flooding) and to enable an optimised interpretation of the results of the analysis (importance and sensitivity).

5 Evaluation of the results

To evaluate the results of a fault tree analysis there are different options:

- minimal-cut-set analysis
- uncertainty and sensitivity analysis
- importance analysis
- time dependent analysis

Before evaluating the results, the legitimate use of these options has to be checked. That means, only if the input parameters are plant specific, actual and verified, all above options are useful and efficient.

6 Variation of parameters and methods

Variations of the input parameters or of the calculation methods are useful to detect principal mistakes in the analysis. The variations are based on the results of the MCS-analysis which show the dominant contributions of the fault trees. Calculations with modified fault trees or different computer-codes have to obtain com
parable results. Different results indicate mistakes or weak points either in the fault tree structure or in the data base.

7 Comparison with other analyses

A comparison of the results of different PSA is difficult because the procedure "PSA" is not exactly defined. Therefore the comparability of the mathematical results must be checked. There are two possibilities to compare the results of different PSA, the overall unavailability and the balance of the design, e.g. the importance and sensitivity of components and the unavailability of safety systems and components. Divergences may indicate mistakes in the analysis, if there are no well founded reasons.

8 Summary

The most common tool to define the reliability of safety systems and components is the fault tree analysis. The results of the calculations enable statements about the reliability of the systems and the influence of the components of the systems. A systematic review is necessary to verify the correctness of complex analysis, especially in case of nuclear power plants. The main points of a fault tree review are check of the fundamentals, of the system analysis and modelling, evaluation of the results, comparison of the results with other analysis and variation of parameters and methods. In general the effort for checking and verifying a fault tree analysis is comparable to the effort of the analysis.

/1/

/2/

/3/

/4/