Logical Trees in Risk Analysis – an Introduction

Nachdiplomkurs Risiko und Sicherheit

Prof. M.H. Faber, February, 2001
Swiss Federal Institute of Technology

Lecture Notes on
Risk and Reliability in Civil Engineering

Basics of Logical Tree Analysis

1. Introduction

Having identified the different sources of risk for an engineering system and or activity and analysed these in respect to their chronological and causal components logical trees may be formulated and used for the further analysis of the overall risk as well as the risk contribution of the individual components.

In the present chapter we will consider the basic aspects of some of the most commonly used types of logical trees, namely fault trees, event trees, cause-consequence charts and decision trees.

Fault trees and event are by far and large the most well-known and most widely applied type of logical tree in both qualitative and quantitative risk analysis. Two of the most important risk studies involving fault tree and event tree analysis were the US nuclear safety study and the UK Canvey study of chemical process industries. Even though more modern risk analysis techniques such as e.g. Bayesian Probabilistic Nets have been developing over the last years fault trees and event trees are still the main methods recommended for US nuclear safety studies.

Fault trees and event trees are in many ways similar and the choice of using one or the other or a combination of both in reality depends more on the traditions and preferences within a given industry than the specific characteristics of the logical tree.

A significant difference between the two types of trees is though that whereas the fault trees take basis in deductive (looking backwards) logic the event trees are inductive (looking forward). In practical applications a combination of fault trees and event trees is typically used where the fault tree part of the analysis in concerned about the representation of the sequences of failures, which may lead to events with consequences and the event tree part of the analysis which is concerned with the representation of the subsequent evolution of the consequence inducing events.
The intersection between the fault tree and the event tree is in reality a matter of preference of the engineer performing the study. Small event tree / large fault tree and large event tree / small fault tree techniques may be applied to the same problem to supplement each other and provide additional insight in the performance of the considered system.

Cause consequence charts incorporate significant features of fault and event trees and are in principal just a combination of the two.

Decision trees are often seen as a special type of event tree, but may in fact bee seen in a much wider perspective and in fact applied consistently within the framework of decision theory provides the theoretical basis for risk analysis.

The detailed analysis of the various types of logical trees requires that the performance of the individual components of the trees already has been assessed in terms of failure rates and or failure probabilities a subject which will not be considered in detail in the present chapter.

2. Fault Tree Analysis

As mentioned previously a fault tree is based on a deductive logic starting by considering an event of system failure and then tries to deduct which causal sequences of component failures could lead to the system failure. The system failure is thus often referred to as a top event.

The logical interrelation of the sequences of component failures is represented through logical connections (logical gates) and the fault tree forms in effect a tree like structure with the top event in the top and basic events at its extremities. The basic events are those events, for which failure rate data or failure probabilities are available and which cannot be dissected further. Sometimes the basic events are differentiated into initiating (or triggering) events and enabling events, where the initiating events are always the firs event in a sequence of events. The enabling events are events, which may increase the severity of the initiated failure.

A fault tree is a Bolean logical diagram comprised primarily of AND and OR gates. The output event of an AND gate occur only if both of the input event occur simultaneously and the output event of an OR gate occur if any one of the input events occur see Figure 1 where different commonly used symbols for AND and OR gates are illustrated.

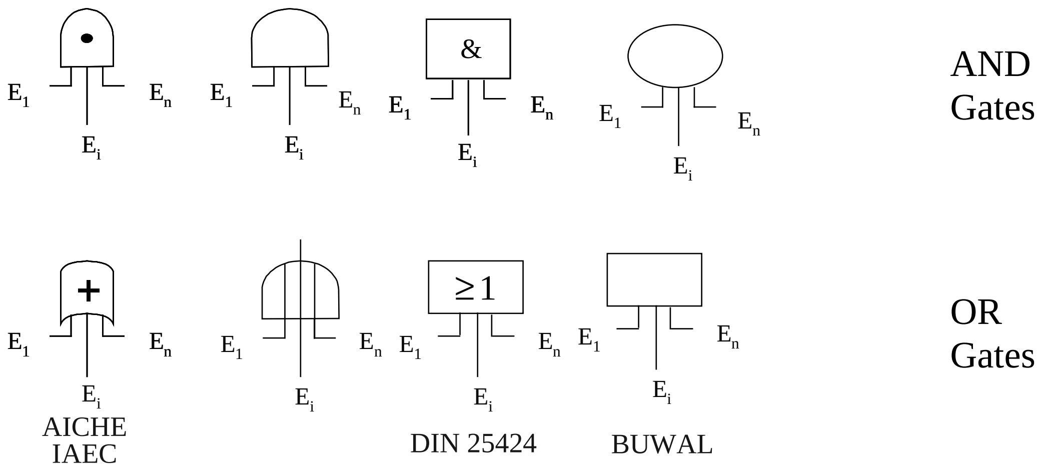

Figure 1 Illustration of commonly used symbols for AND and OR gates. Several other types of logical gates exists such as e.g. DELAY, MATRIX, QUANTIFICATION and COMPARISON, however, these will not be elaborated in the present text.

Top events and basic events also have their specific symbols as shown in Figure 2.

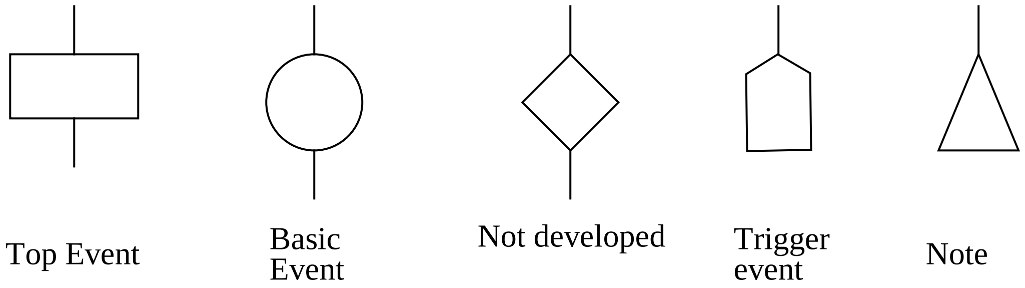

Figure 2 Symbols commonly used in fault tree representations.

In Figure 2 the diamond shaped symbol represents an undeveloped scenario which has not been developed in to a system of sub events due to lack of information and data.

An example of a fault tree is shown in Figure 3.

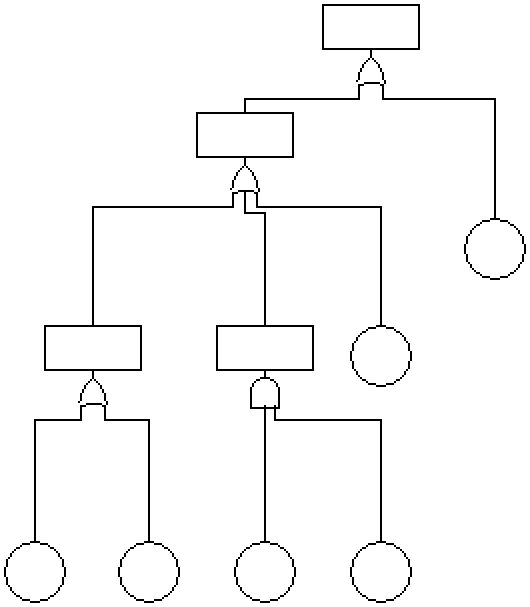

Figure 3 Principal shape of a fault tree.

It is noted that a fault tree comprising an AND gate represents a parallel system, i.e. all components must fail for the system to fail. Such a system thus represents some degree of redundancy because the system will still function after one component has failed. Fault trees comprising an OR gate on the other hand represents a series system, i.e. a system without any redundancy in the sense that it fails as soon as any one of its components has failed. Such as system is also often denoted a weakest component system. Such systems may thus be represented alternatively by reliability block diagrams, see Figure 4.

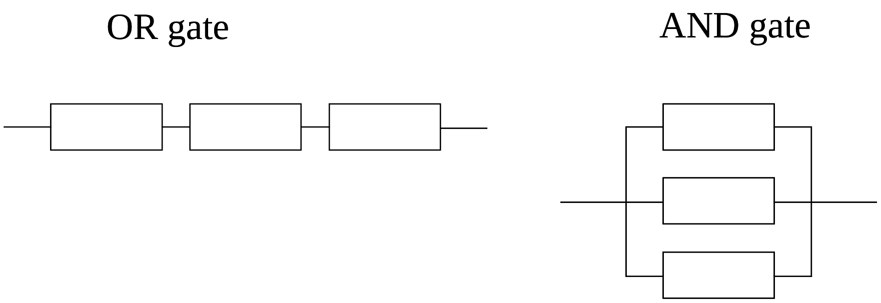

Figure 4 Reliability block diagrams for OR and AND gates.

In accordance with the rules of probability theory the probability of the event for an AND gate is evaluated by

$$P = \prod_{i=1}^{n} p_i \tag{1}$$

and for an OR gate by

$$P = \sum_{i=1}^{n} p_i - \sum_{i,j=1,i\neq j}^{n} p_i p_j \tag{2}$$

where n is the number of ingoing event to the gate and it is assumed that the ingoing events are independent.

System failure modes are defined by so-called cut-sets, which are combinations of basic events, which with certainty will lead to the top event. The number of such combinations can be rather large event several hundreds for a logical tree with about 50 basic events. It is important to note that the top event may still occur event though not all basic events in a cut set occur. A minimal cut set is the cut set that represents the smallest combination of basic events leading to the top event, sometimes denoted the critical path. The top event will only occur if all events in the minimal cut set occur. An important aspect of fault tree analysis is the identification of the minimal cut sets as this greatly facilitates the numerical evaluations involved.

As an example consider the following simple risk analysis.
Consider a power supply system composed of an engine, a main fuel supply for the engine and electrical cables distributing the power to the consumers. Furthermore as a backup fuel support a reserve fuel support with limited capacity

is installed. The power supply system fails if the consumer is cut of from the power supply. This in turn will happen if either the power supply cables fail or the engine stops, which in turn is assumed only to occur if the fuel supply to the engine fails.

A fault tree system model for the power supply is illustrated in Figure 5. In Figure 5 also the probabilities for the basic events are illustrated.

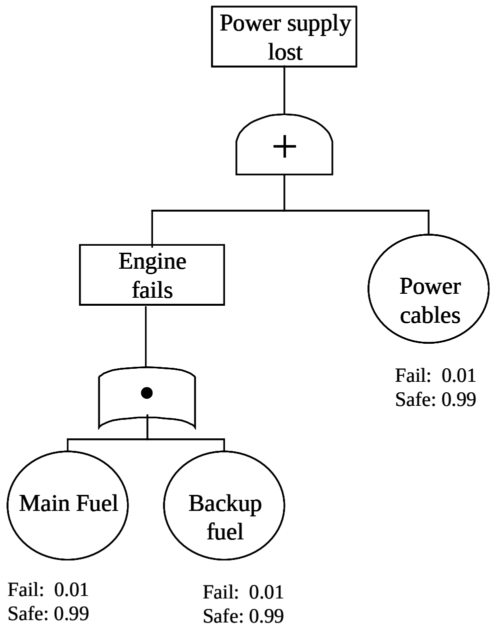

Figure 5 Illustration of a fault tree for a power supply system.

Using the rules of probability calculus we obtain that the probability of engine failure P_{EF} is equal to (AND gate)

$$P_{EF} = 0.01 \cdot 0.01 = 0.0001$$

along the same lines we obtain that the probability of lost power support P_{PF} is equal to (OR gate)

$$P_{PF} = 0.0001 + 0.01 - 0.0001 \cdot 0.01 = 0.0101$$

3. Event trees

An event tree is a representation of the logical order of events leading to some (normally adverse) condition of interest for a considered system. It should be noted that several different states for the considered system can be associated with important consequences.
In contrast to the fault tree is initiates with a basic initiating event and develops from there in time until all possible states with adverse consequences have been reached. The initiating events may typically arise as top events from fault tree analysis. The event tree is constructed from event definitions and logical vertices (out comes of events), which may have a discrete sample space as well as a continuous sample space. Typical graphical representations of event trees are shown in Figure 6.

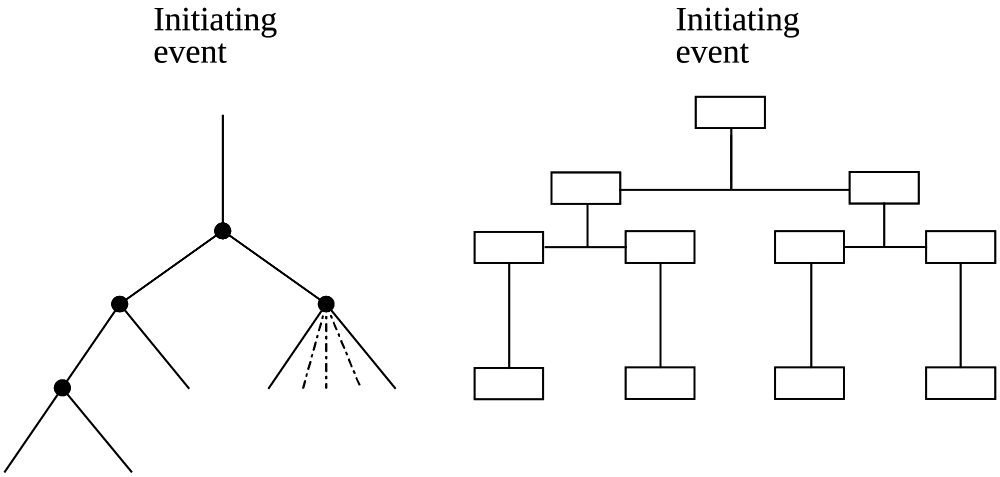

Figure 6 Illustration of the principal appearance of an event tree.

Event trees can become rather complex to analyse. This is easily realised by noting that for a system with n two-state components the total number of paths is 2^n. If each component has m states the total number of branches is m^n.

An example of an event tree is shown in Figure 6. The event tree models the event scenarios in connection with non-destructive testing of a concrete structure. Corrosion of the reinforcement may be present and the inspection method applied may or may not detect the corrosion, given corrosion is present and given that corrosion is not present.

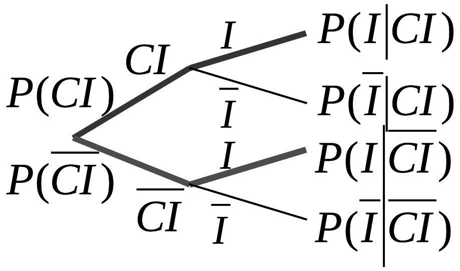

Figure 7 Illustration of event tree for the modelling of inspection of a reinforced concrete structure.

In Figure 7 the events CI denote that corrosion is present, and I that the corrosion is found by inspection. The bars over the events denote the complementary events. On the basis of such event trees e.g. the probability that corrosion is present given that it is found by inspection may be evaluated.

In many cases the event trees may be reduced significantly after some preliminary evaluations. This is e.g. the case when it can be shown that the branching probabilities become negligible. This is often utilised e.g. when event trees are used in connection with inspection and maintenance planning. In such cases the branches corresponding to failure events after repair events may often be omitted at least for systems with highly reliable components.

In Figure 8 a combined fault tree and event tree is illustrated showing how fault trees often constitute the modelling of the initiating event for the event tree.

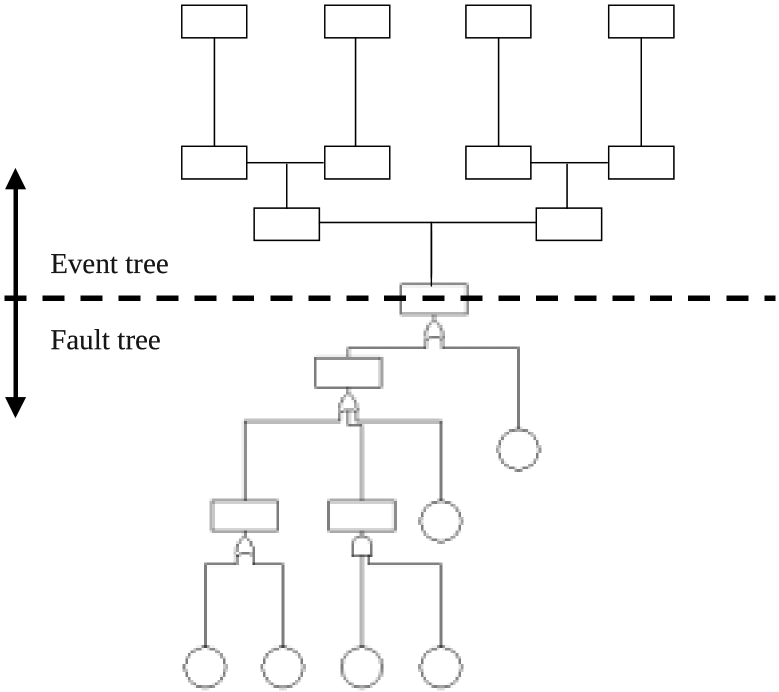

Figure 8 Illustration of combined fault tree and event tree.

4. Cause Consequence Charts

Cause consequence charts are in essence yet another representation of combined fault trees and event trees in the sense that the interrelation between the fault tree and the event tree namely the top event for the fault tree (or the initiating event- for the event tree) is represented by a rectangular gate with out put event being either YES or NO, each of which will lead to different consequences. The benefit of the cause consequence chart being that the fault tree need not be represented in the representation, enhancing the overview of the risk analysis greatly.

An example of a gate in a cause consequence chart is shown in Figure 9.

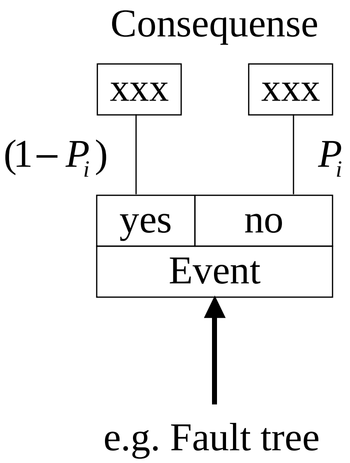

Figure 9 Gate in a cause consequence chart.

5. Decision trees

As already mentioned decision trees applied within the framework of the decision theory form the basic framework for risk analysis. This may be realised by recognition of the fact that risk analysis serves the purpose of decision-making. Either the risk analysis shows that the risks are acceptable and one does nothing, or it is found that the risks are not acceptable and one has to do something. The decision analysis is the framework for the assessment of the risks as well as for the evaluation of how to reduce the risks most efficiently.

In the following we will not go into the details of the decision theory, which will be elaborated in a later chapter. Here we will only discuss the principal characteristics of the decision tree. An example of a decision tree is shown in Figure 10.

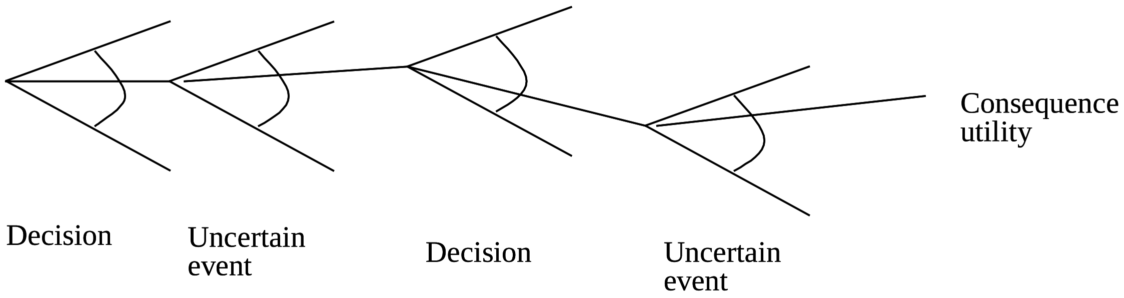

Figure 10 Principal representation of a decision tree

The decision tree is constructed as a consecutive row of decisions followed by uncertain events thus reflecting the uncertain out come of the possible actions, which may be follow from the decisions. In the end of the decision tree consequences or utilities are assigned in accordance with the decisions and the out comes of the uncertain events. Depending on the number of decisions and or actions involved in the decision analysis and thus represented in the decision tree various types of decision analysis are required, ranging from the most simple so-called prior decision analysis to the most advanced pre-posterior analysis.

It is important to note that the probabilities for the different events represented in the decision tree may be assessed by fault tree analysis, event tree analysis, structural reliability analysis or any combination of these and thus the decision tree in effect includes all these aspects of systems and component modelling in addition to providing a framework for the decision making.