Module 7

Logical Trees

Different sources of risk for an engineering system and / or activity can be analyzed with respect to their chronological and causal components using logical trees. They are useful for the analysis of the overall risk as well as for the assessment of the risk contribution from the Individual components.

Fault tree and event tree diagrams are the most well known and most widely applied type of logical trees in both qualitative and quantitative risk analysis. Even though more modern risk analysis techniques such as eg. Bayesian probabilistic nets have been developed over last years, fault tree and event tree are still main methods recommended (for US nuclear safety studies). Fault trees and event trees are in many ways similar and the choice of using one other or a combination of both in reality depends more on the traditions/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 the fault trees take basis in deductive (looking backwards) logic and the event trees are inductive (looking forward). In practical applications, a combination of fault trees and event trees is typically used. In this case, the fault tree part of the analysis is concerned about the representation of the sequences of failures, which may lead events with consequences and the event tree part of the analysis is concerned with the representation of the subsequent evolution of the consequence inducing events.

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 with regard to the reliability of the considered system.

Decision trees are often seen as a special type of event tree, but may be seen in much wider perspective and if applied consistently within the framework of decision theory, provide 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.

7.1. Fault Tree Analysis

As mentioned earlier a fault tree is based on a deductive logic starting by considering an event of system failure and then aims to deduct which causal sequence of component failures could lead to the system failure. The system 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 events are differentiated into initiating (or triggering) events and enabling events, where the initiating events are always the first event in a sequence of the enabling events are events, which may increase the severity of the initiated failure.

The fault tree is a Boolean logical diagram comprised primarily of AND and OR gates. The output event of an AND gate occurs only if all of the input events occur simultaneously and the output event of an OR gate occur if any one of the input occurs. Figure 1 illustrates different commonly used symbols for AND and OR gates.

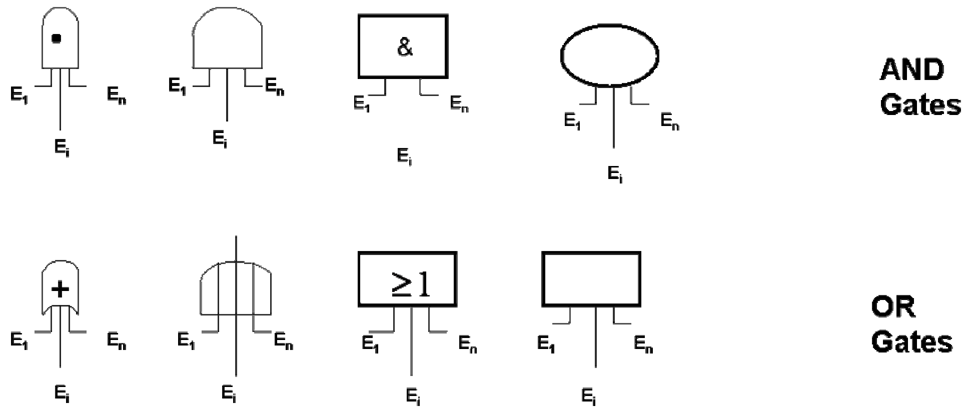

Figure 1 – Illustration of commonly used symbols for AND and OR gates

Several other types of logical gates exists such as QUANTIFICATION and COMPARISON, however, these will not be elaborated in present text.

Top events and basic events also have their specific symbols as shown in figure below

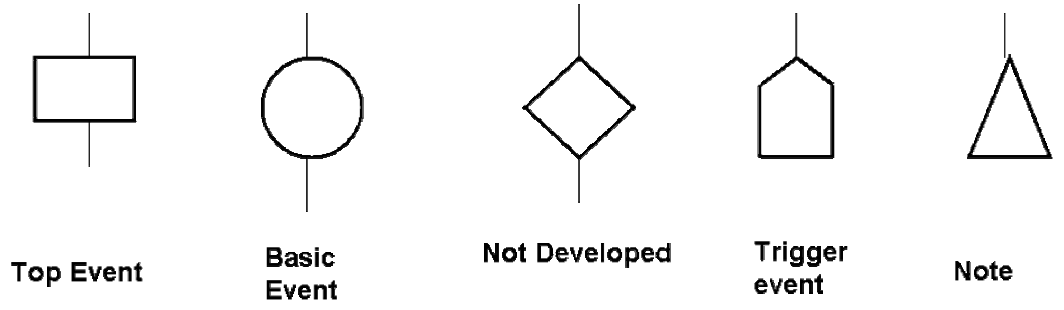

Figure 2 – Symbols commonly used in fault tree representations

In the Figure 2 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.

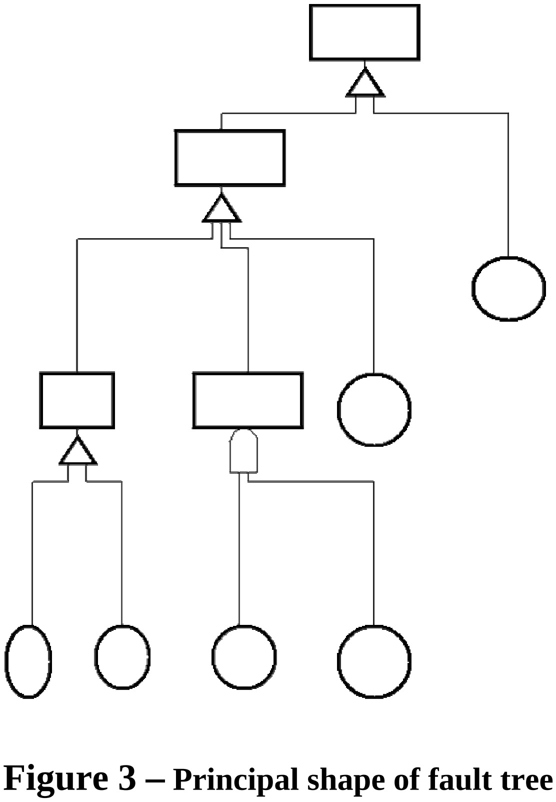

Figure 3 – Principal shape of fault tree

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 often denoted a weakest component system. Systems may be represented alternatively by reliability block diagrams, see Figure 4.

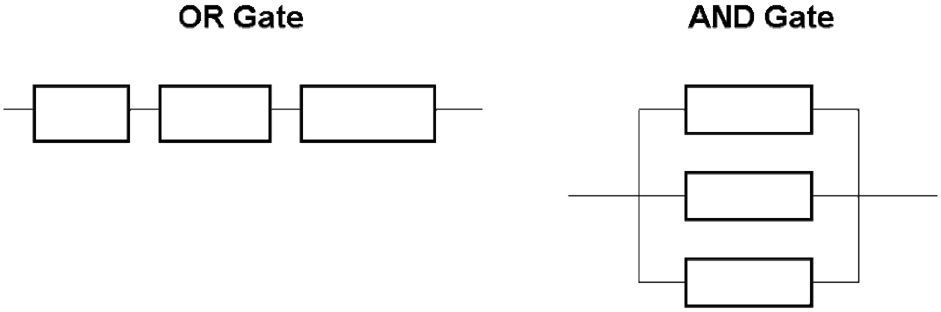

Figure 4 – Reliability block diagrams for OR and AND gates

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

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

And for an OR gate by

$$P = 1 - \prod_{i=1}^{n} (1 - p_i)$$

Where n is the number of ingoing event to the gate .P_i are the probabilities of the failure of ingoing events and it is assumed that the ingoing are independent.

System failure modes are defined by so-called cut-sets, i.e. combinations of basic events, which with certainty will lead to the top event. The number of such combinations can be rather large - 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 die 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.

7.2. 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 could be associated the important consequences.

In contrast to the fault tree it starts from 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 (outcomes 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 5.

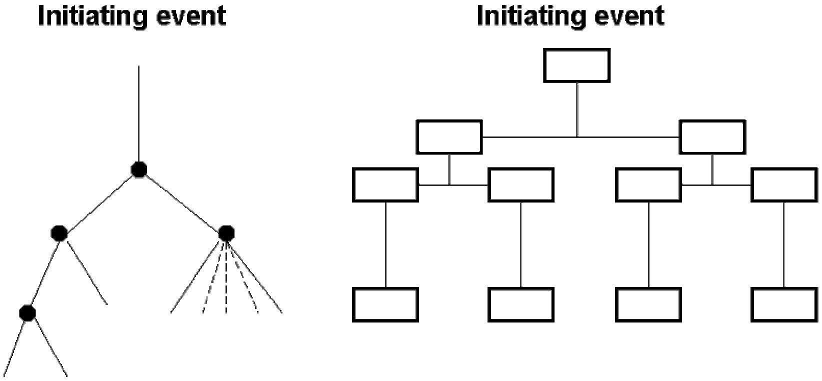

Figure 5 – Illustration of the principal appearance of an event tree

Event trees can become rather complex to analyze, This is easily realized 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.

7.3. 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 output event being either YES or NO, each of which will lead to different consequences. The benefit of the cause consequence chart is that the fault tree need not be expanded 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 6.

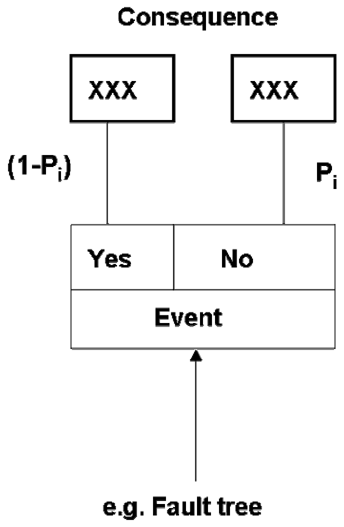

Figure 6 – Gate in a cause consequence chart

7.4. Decision trees

As already indicated, decision trees applied within the framework of the decision theory form the basic framework for risk analysis. This may be realized 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. An example of a decision tree is Figure 7

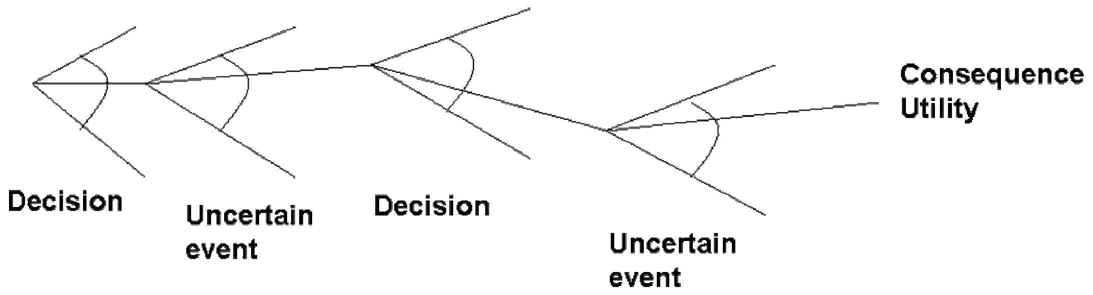

Figure 7 – Principle representation of a decision tree

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 may follow from the decisions. In the end of the decision tree, consequences (or utilities) are assigned in accordance with the decisions and the outcomes of the uncertain events. Depending on the number of decisions and or action 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, reliability analysis or any combination of these and thus the decision tree in effect includes all these aspects of systems and component modeling in addition to providing a framework for the decision making.