Safety Reliability Risk Assessment: Fault Tree Construction

An Online Continuing Education Course for Engineers

Course Number: M-3056

Credit: 3 Hours / 3 PDH / 3 CPD

Safety-Reliability-Risk Assessment: Fault Tree Construction

C. Sundararajan, Ph.D., MASCE, FASME

COURSE OUTLINE

1. INTRODUCTION

Fault tree analysis is one of the most widely used methods for system reliability analysis. It is a formal deductive procedure to determine the various combinations of component-level failures that could result in the occurrence of specified "undesired events" at the system-level. Not only hardware (component) failures but also human errors and software errors are considered "component-level failures", within the context of fault tree construction and analysis. The undesired event could be an accident, unscheduled/forced shutdown or other system-level failures. Fault trees may also be used to compute the probability of the undesired event as a function of the probabilities of component failures. We may construct a number of fault trees for the same system if we are interested in studying a number of undesired events relating to that system. Each undesired event would have a different fault tree.

We use the term "failure" here to refer to both "failures" and "faults". Definition of fault and failure are provided and discussed in Appendix 1.

Fault trees may be constructed at any stage of system design. If a fault tree is constructed at an early stage of system design, it may be updated as more precise information become available or changes are made in the design. Fault trees may also be constructed for operating systems to identify the root causes of system-level failures encountered during operation.

A fault tree analysis may follow a preliminary hazard analysis (Sundararajan 2008) or a failure modes and effects analysis (Sundararajan 2008) although neither a preliminary hazard analysis nor a failure modes and effects analysis is a prerequisite.

A full fault tree analysis consists of

1. Fault tree construction,

2. Qualitative fault tree analysis, and

3. Quantitative fault tree analysis (a quantitative analysis may be performed without first performing a qualitative analysis).

Depending on the scope of the reliability project, either steps 1 and 2, or steps 1 and 3, or steps 1, 2 and 3 may be performed.

We discuss fault tree construction in this course. Qualitative analysis and quantitative analysis will be discussed in future courses.

We start the course by developing a fault tree for a simple electrical system in Section 2. This example illustrates how a system level failure can be resolved to component level failures via a fault tree. Concept of gates and events are also introduced through this example. System description is discussed next in Section 4. A system description helps in the construction of fault trees, especially,

for large complex systems. Section 4 presents the symbols used to represent the various gates and events in fault trees. Detailed descriptions and discussion of the various gates are provided in section 5; illustrative examples are given when necessary. Different types of events used in fault trees and different types of component failures are discussed at some length in Section 6. An eight-character (eight-digit) naming system for uniquely identifying every terminal event in a tree is also presented and illustrated in that section. Transfer symbols used in the display of large fault trees are discussed in section 7. Common cause failures and their representation in fault trees is the subject of Section 8. Section 9 describes the construction of complementary trees (also known as success trees). Limitations of fault trees and documentation of fault tree construction are discussed in Section 10 and 11, respectively. Section 12 discusses how fault trees are used in quantitative and/or quantitative fault tree analyses. Course ends with the construction of fault tree for an example domestic hot water system (DHWS).

Before we go into fault tree construction, a word of caution is in order. If two reliability analysts develop fault trees for the same undesired event of a system, the two fault trees may not necessarily be identical; they may seem different at the outset, particularly if the system is complex. This is because the way in which system logic is modeled by the two analysts may differ. However, the two fault trees must provide the same results when a qualitative and/or quantitative analysis is carried out.

2. AN EXAMPLE FAULT TREE

Fault tree is a graphic representation of the relationship between component-level failures and a system-level undesired event. It depicts how component-level failures propagate through the system to cause a system-level failure or some system-level undesired event. The component-level failures are called the terminal events, primary events or end events of the fault tree; we will mostly use the term "terminal event" is this course module. The system-level undesired event is called the top event of the fault tree.

The concept of fault trees is best explained through a simple illustration. We have purposively chosen a very simple example; fault trees encountered in practice could be tens or hundreds of time larger than this simple illustration.

A system diagram for the operation of an electric motor is shown in Figure 1. We are interested in developing a fault tree for the undesired event "motor overheats". The fault tree is shown in Figure 2. Let us discuss how we draw that fault tree.

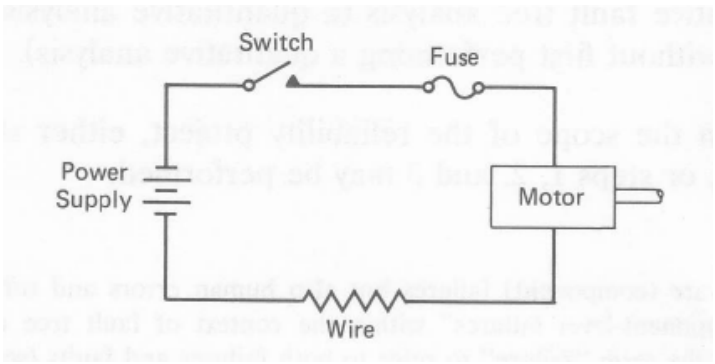


Figure 1: System diagram for the operation of an electric motor.

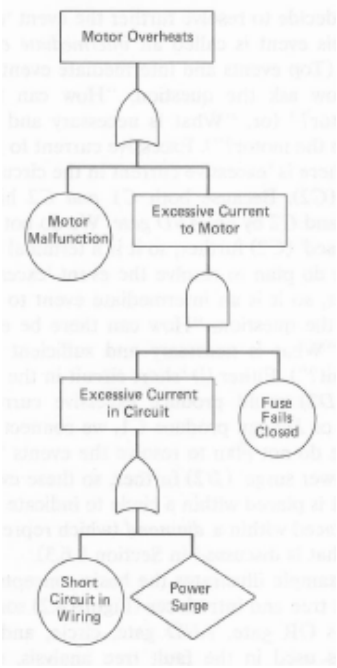
First, we place the undesired event at the top of the tree within a rectangle (General convention is to use a rectangle to represent Top Event). The undesired event, in this case, is "motor overheats". For the sake of simplicity in further discussions, let us denote it by the symbol A. Next, we ask the question: "how can the motor overheat?" (or, "what is necessary and sufficient for the motor to overheat?"). Motor overheating can happen (i) due to an internal malfunction of the motor itself, or (ii) due to excessive current supplied to the motor. So we place the events "motor malfunction" and "excessive current to motor" below the top event (undesired event). Let us denote these events by B1 and B2, respectively. Since A is possible either by “motor overheating” (B1) or by “excessive current” (B2), we connect A to B1 and B2 by an "OR gate".

At this point, we may either explore the reasons for "motor malfunction" (B1) by examining the failures of the various parts of the motor or treat "motor malfunction" as a terminal event (component-level failure). In this example, we choose to do the latter. So we place the event "motor malfunction" within a circle to indicate that it is a terminal event. (Convention is to use a circle to represent Terminal Event.) Criteria for deciding whether to treat an event as a terminal event or not is discussed later in Section 6.3.

We decide to resolve further the event "excessive current to motor" (B2). So this event is called an intermediate event, and is placed within a rectangle. (Top events and intermediate events are placed within rectangles). We now ask the question: "how can there be excessive current to the motor?" (or, "what is necessary and sufficient to cause excessive current to the motor?") Excessive current to the motor (B2) can happen only if (i) there is "excessive current in the circuit" (C1) and (ii) the "fuse fails closed" (C2). Since both C1 and C2 have to happen, we connect B2 to C1 and C2 by an "AND gate". We do not plan to explore the event "fuse fails closed" (C2) further, and so it is a terminal event and placed within a circle. We do plan to resolve the event "excessive current in the circuit" (C1) further, and so it is an intermediate event to be placed within a rectangle.

We ask the question: "how can there be excessive current in the circuit?" (or, "what is necessary and sufficient to cause excessive current in the circuit?"). Either (i) "shortening of the wiring" (D1) or (ii) a "power surge" (D2) could produce excessive current in the circuit. Since either D1 or D2 can produce C1, we connect C1 to D1 and D2 by an "OR gate". We do not plan to resolve the events

"shortening of the wiring" (D1) or "power surge" (D2) further. So these events are treated as terminal events. D1 is placed within a circle to indicate that it is a terminal event, and D2 is placed within a diamond (a diamond represents a special type of terminal event which is discussed in Section 6.3).



Motor overheats - A (Top Event)
Motor malfunction - B1 (Terminal Event)
Excessive current to motor - B2 (Intermediate Event)
Excessive current in the circuit - C1 (Intermediate Event)
Fuse fails closed - C2 (Terminal Event)
Shortening of the wiring - D1 (Terminal Event)
Power surge - D2 (Undeveloped Terminal Event - discussed in Section 6.3)

Figure 2: Fault tree for “motor overheats”

The above example illustrates the basic concepts and procedure of constructing a fault tree. Some symbols used in fault trees, such as, OR gate, AND gate, rectangle, circle and diamond are also introduced (Figure 2). Some terms used in the fault tree analysis, such as top event, intermediate event, terminal event, OR gate and AND gate, are also defined. A number of other symbols and terms are defined in later sections of this course. Fault tree for a somewhat complex system is developed in Section 13.

3. SYSTEM DESCRIPTION

Within the context of fault tree analysis, one may consider a complete plant as a system or some

distinct parts of a plant as a system (for example, steam generation system, emergency cooling system, distillation system, feed water system, emergency power supply system, etc.), or even an equipment may be treated as a system.

The first step in any reliability analysis, including fault tree analysis, is to understand the system well. A clear understanding of the system, as it pertains to the fault tree, is necessary. Detailed information about each and every component in the system, the functional and physical interconnections between components, the normal and abnormal environments experienced by each component, and failure modes of each component are gathered from drawings, schematic diagrams, block diagrams, logic diagrams, piping and instrumentation diagrams, process flow sheets, installation diagrams, parts lists, operating procedures, maintenance-test procedures, discussions with plant personnel, etc. In addition, interfaces of the system with other systems (for example, power supply system, cooling water supply system, etc.) should be identified.

The reliability analyst may prepare a system description, which includes the following information.

1. List of components (Note that some components may be part of more than one system since system boundaries may overlap),

2. Physical interconnections and proximity of components, and

3. Physical interfaces with other systems.

The system may function in more th e, normal operating mode, emergency operating mod ional test mode, etc. Only a few of the functiona nctional description may be prepared for each fu shall include the following information:

1. Function of each

2. Initial conditions is empty or full, motor is operating or idle, etc.),

3. Functional interfa

4. Normal operating (temperature, pressure, humidity, mechanical str

5. Abnormal operatin during emergency or accidental conditions,

6. Failure modes of ea ve fails open, valve fails closed, pipe break, pipe leak,