Chapter 2
An Overview of System Safety Assessment

Abstract This chapter provides an introduction to the steps involved in creating dependable systems. This starts with a description of functional hazard assessment (FHA). The steps involved in preliminary system safety assessment (PSSA) and system safety assessment (SSA) are reviewed. The chapter introduces fault tree analysis (FTA) and failure modes and effects analysis (FMEA) as important tools in the safety assessment process. This chapter also introduces the basics of probability theory which can guide quantitative assessment. The concepts behind common cause analysis are introduced. To make the book self-contained, more detailed mathematical concepts are presented in the appendices which can be skipped by less mathematically inclined readers.

Introduction

Chapter 1 described the properties of dependable systems. This chapter introduces systematic methods used in the design and development of dependable systems. Industries such as nuclear, aviation, railways, and their regulatory agencies have over the years developed standards, analytical techniques for safety assessment with interdisciplinary applications which will be introduced in this chapter. These are the methods which are used in system design when a new product or service is conceived.

This chapter borrows heavily from the aerospace industry which has amongst the most rigorous standards. An important guiding document for safety in development of new aircraft is ARP 4761 [1]. *The methods employed are qualitative*, *quantitative, or both*. These include functional hazard assessment (FHA), failure modes and effects analysis (FMEA), fault tree analysis (FTA), dependence diagrams (DD), Markov analysis (MA), and common cause analysis (CCA) (which is composed of zonal safety analysis (ZSA), particular risks analysis (PRA), and common mode analysis (CMA)).

The development process is iterative in nature with system safety being an inherent part of the process. The process begins with concept design and derives an initial set of safety requirements for it. During design development, changes are made to it and the modified design must be reassessed to meet safety objectives. This may create new design requirements. These in turn necessitate further design

N. Balakrishnan, *Dependability in Medicine and Neurology*,
DOI 10.1007/978-3-319-14968-4_2

changes. The safety assessment process ends with verification that the design meets safety requirements and regulatory standards [1]. The safety assessment process begins with FHA, preliminary system safety assessment (PSSA), and system safety assessment (SSA). These techniques are applied iteratively. Once FHA is performed, PSSA is performed to evaluate the proposed design or system architecture. The SSA is performed to evaluate whether the final design meets requirements.

The subject matter in this chapter can be initially challenging. The reader is encouraged to skim the contents at first glance and proceed to subsequent chapters which elaborate on the concepts described here in a medical framework and return frequently to reinforce concepts.

Functional Hazard Assessment

FHA is performed at the beginning of system development. Its main objective is to "identify and classify failure conditions associated with the system by their severity" [1]. The identification of these failure conditions is vital to establish the safety objectives. This is usually performed at two levels, for the example of the aircraft industry—at the completed aircraft level and at the individual system level [1].

The aircraft level FHA identifies failure conditions of the aircraft. The system level FHA is an iterative qualitative assessment which identifies the effects of single and combined system failures on aircraft function. The results of the aircraft and system level FHA are the starting point for the generation of safety requirements. Based on this data, fault trees, FMEA can be performed for the identified failure conditions which are studied later.

ARP 4761 provides guidelines on how an FHA should be conducted. Since this is an iterative process, it is performed in broad categories with increasing resolution as the analysis proceeds to finer and finer subsystems. A recommended manner to accomplish this is to list all the performance requirements based on design characteristics. Once the high-level requirements have been identified, the failure conditions associated with them are identified. This is then used to generate lower level requirements. This process is then applied iteratively till the design is complete. An illustrative example for aircraft is as shown below:

Aircraft function	Failure condition
1. To control aircraft trajectory	Loss of aircraft control
	Loss of pitch control (partial control loss)
	Runaway of one control surface

These failure conditions are further broken down in a systematic manner through FHA performed at the system level. FHA therefore is a top-down process; it proceeds from the broad to more specific functions and their failures. The following steps are involved [1]:

Determine and Characterize Inputs at Product Level or System Level

For an aircraft this involves specification of top level functions such as passenger load, thrust, lift, customer requirements, etc. For an automobile, this involves description of the type of vehicle (sedan, minivan, etc.), performance requirements such as horsepower, torque, braking, steering; control systems, transmission, safety systems. For individual systems such as braking, system level approach involves looking at subsystems such as hydraulics, interface with electronic control systems such as antilock braking system (ABS), power brakes, and so on.

FHA Process

Once the inputs (as above) have been identified, the following steps are then applied.

- Identify all the functions with the level under study [1]. These include functions provided by the system and all the other systems interlinked to the system under study.
- Identify and describe failure conditions associated with these functions, considering single and multiple failures under different conditions [1]. Examples include "loss of hydraulics" under "normal weather" or "ice/snow storm" conditions.
- Determine the effects of the failure conditions.
- Classify failure condition effects. This is shown in Chap. 1, Table 1.1. Common classification systems in use across several domains (aviation, railway) are catastrophic (e.g., loss of engines), severe, major, hazardous, minor, and no safety effect (e.g., loss of in-flight entertainment system). Based on failure condition classification, allowable probability limits of occurrence and required developmental assurance levels (DAL) are assigned as described in Chap. 1.
- Assignment of requirements to the failure conditions at the next lower level of analysis. Why is this failure catastrophic or why is it only minor? Identify supporting materials for failure condition effect classification. This can be from simulations, prior experience with similar aircraft, etc.
- Identify methods used to verify compliance with failure condition requirements.

A careful examination of the above method shows that a good FHA is a collaborative, multidisciplinary effort requiring great domain knowledge and insight requiring great qualitative effort. The FHA leads to the PSSA.

FHA in Neurological Diagnosis and Treatment

FHA is a very useful method for analyzing and mitigating morbidity from medical illness, especially neurological illness. In cases where the underlying disease is not directly treatable, FHA is a systematic method for identifying the morbidity from the untreatable illness. The underlying disease causes loss of normal function or permits gain of abnormal function both of which cause significant distress to the patient. Examples of loss of function include weakness, poor balance, difficulty swallowing, and difficulty speaking, etc. Examples of gain of function include severe pain from neuropathy, painful myositis, etc. The failure classification helps quantify the clinical significance of the change in function. Painful neuropathy, through distressing and leading to a poor quality of life would not be expected to shorten life expectancy or cause significant problems with mobility. Therefore this can be classified as minor. Difficulty swallowing on the other hand can lead to progressive weight loss and aspiration which can be fatal. Therefore this failure condition can be classified as major or catastrophic. This helps direct resources and plan treatment costs appropriately. The following case examples are illustrative.

Case Example 1

J.C.C. is a 75-year-old avid saxophone player. He noticed insidious onset of loss of dexterity in his left hand while playing the saxophone for the last several months. He denied any abnormal posturing or pain in the left upper extremity while playing the saxophone. He reported that he was unable to seamlessly move between octaves and was unable to initiate fine movements with his fingers for precise playing of certain rhythms. He denied any pain, numbness, or weakness in the left upper extremity. He had not noticed any loss of dexterity with less challenging tasks such as manipulating a fork and knife while eating. He denied any symptoms in his right upper extremity.

He reported sleep problems with a tendency to sleep walk and sustained a fracture in his right little finger approximately a year ago while possibly acting out his dreams during sleep. He denied any significant changes in smell. He denied any falls. He also denied any visual hallucinations or memory loss. He had noticed some twitching, which may actually resemble a tremor in the left upper extremity, but this was very infrequent. He denied any memory problems or cognitive

difficulties and remained actively involved in the stock market with surprisingly good returns. However he reported severe depression for the last several years.

On examination, mental status and cranial nerve examination were normal save decreased blink rate and facial expression. He had significant diffuse bradykinesia. He had normal 5/5 strength in his bilateral upper extremities without evidence of fasciculations or atrophy. He also had reduced ability to tap his fingers on the left side when compared to the right. Examination of motor tone revealed left upper extremity cogwheel rigidity, exacerbated by exercising his right upper extremity. He had normal tone in the right upper and bilateral lower extremities. Gait examination revealed a festinant gait without retropulsion. There was no evidence of apraxia. Based on this history, physical examination, a diagnosis of Parkinson's disease was made. FHA of J.C.C. reveals the following:

Normal function	Failure condition
1. Fine motor control of fingers of left hand	1. Partial loss of fine motor function of left hand
2. Speed and rhythm of movement	2. Partial slowing of movement in all limbs
3. Normal mood and cheer	3. Severely depressed mood and cheer
4. Normal sleep	4. REM behavior disorder

The FHA can guide therapy. In J.C.C.'s case, treatment of depression with citalopram and REM behavior disorder with clonazepam had the greatest impact on his life. He did not tolerate levodopa well and had a modest response to pramipexole which enabled him to continue his hobby for several more years.

Case Example 2

S.C. is a 61 y/o male who developed bilateral shoulder pain, soreness 5–6 weeks ago. Subsequently he developed shortness of breath, especially when lying down. Symptoms are worst during the night when he wakes severely dyspneic after 3–4 h of sleep. Most routine activities during the day are well tolerated; however he would get severely short of breath with minor exertion. He denied any changes in his vision, any difficulty chewing or swallowing. He also denied any weakness elsewhere or any changes in sensation or bladder function. He denied any antecedent vaccinations, flu-like illnesses or tick bites. He was evaluated by his pulmonologist who noticed high diaphragms on a chest X-ray that was performed as part of routine evaluation. On examination, he had normal mental status, cranial nerves, extremity strength, sensation, and mildly brisk symmetric reflexes with downgoing toes. He was severely orthopneic with paradoxical movements of the diaphragm and observed to need accessory muscles of respiration like the sternocleidomastoid. NCS/EMG showed normal nerve conduction studies and fibrillations and positive sharp waves in the diaphragm with a complete absence of any recruitable motor

units. Based on his clinical, radiographic, and EMG findings he was diagnosed with bilateral diaphragmatic palsy, likely as a consequence of idiopathic brachial neuritis (Parsonage Turner syndrome) because of prodromal shoulder pain. MRI Cervical Spine, spinal fluid studies were normal and an empirical trial of intravenous immunoglobulin (IVIG) and prednisone did not yield any benefit. CT Chest and neck excluded any mass lesions infiltrating the phrenic nerves. FHA helped mitigate his diaphragmatic failure condition.

Normal function	Failure condition
1. Ventilatory function during daytime	1. Partial loss of ventilatory function during daytime (especially exertion)
2. Ventilatory function during nighttime	2. Severe loss of ventilatory function at night time

Based on the results of overnight pulse oximetry, he was started on night time BiPAP with adequate restoration of quality of life. Further pharmacotherapy with repeat IVIG, prolonged steroid therapy or other immunosuppression was not performed.

Case Example 3

D.B.S. is a 60 y/o male presenting with numbness, tingling, and painful paresthesias involving his toes for the last several months. Symptoms started in the right lower extremity, experienced most towards the great toe followed by involvement of the left lower extremity 6 months later. Symptoms are worse when wearing tight shoes, standing and walking for prolonged periods. Feet would feel hot or experience a pressure like discomfort. He denied any urinary, bowel disturbances. He also denied dry eyes and dry mouth. He experienced back trauma in the 1990s which was monitored nonoperatively. Symptoms are not experienced at rest, especially at night. He felt mild involvement of the hands at the time of his appointment. He denied any neck pain. He had an extensive evaluation through his primary care physician which excluded diabetes mellitus and vitamin deficiency. Physical examination revealed normal strength and reflexes down to the ankles. Sensory examination revealed normal joint position sense, mild loss of distal pinprick sensation involving the feet. A nerve conduction study revealed mild demyelinating features suggestive of distal acquired demyelinating symmetrical (DADS) variant of chronic inflammatory demyelinating polyneuropathy (CIDP). Blood work revealed a faint IgM Lambda spike. Follow-up testing revealed very high titers of anti-myelin-associated glycoprotein (anti-MAG) antibodies which frequently causes such a presentation. Therapeutic approaches to the anti-MAG syndrome are very challenging ranging from IVIG, plasmapheresis, steroids, and rituximab [2]. FHA yields the following:

Normal function	Failure condition
1. Normal perception in feet	1. Partial loss of normal sensation in the feet 1.1 Partial loss of skin sensation in the feet
2. Absence of abnormal sensation like tingling, pain involving feet	2. Moderate pain and tingling involving feet
3. Normal serum protein profile in blood	3. Abnormal IgM Lambda spike on serum immunofixation

Since the therapeutic choices are so varied and so expensive, FHA is very useful in guiding therapy.

Given the mild failure conditions observed on FHA, immunotherapy for CIDP was deferred. The patient experienced very little clinical progression despite abnormal test results over 2 years. At the end of 2 years he was placed on Gabapentin 300 mg once to twice daily for symptomatic relief of moderate pain and tingling involving the feet.

Preliminary System Safety Assessment

PSSA is a systematic examination of the proposed system architecture to examine how failures can lead to the functional hazards identified by the FHA and how safety requirements can be met [1]. The PSSA addresses each failure condition identified by the FHA in qualitative or quantitative terms [1]. It involves the use of tools such as FTA, DD, and MA to identify possible faults. The use of these is discussed later. The identification of hardware and software faults and their possible contributions to various failure conditions identified in the FHA provides the data for deriving the appropriate DAL for individual systems. The process is iterative being performed at the aircraft level (for the case of airplanes) followed by individual system levels. The process involves the following steps [1, 3]:

Inputs to PSSA

Aircraft level FHA, System level FHA.

PSSA Process

The PSSA is a top-down process which determines how system failures can lead to the functional impairments or failures identified by the FHA. The following steps are involved in performing a PSSA for the example of aircraft [1]:

1. *Identify and list aircraft and system level safety level requirements*:
   This is derived from the FHA and preliminary CCA (common cause analysis, discussed in detail below in Section "Common Cause Analysis (CMA, ZSA, and PRA)") processes which create the initial safety requirements for the systems. This information is combined with the knowledge of system architecture and performance features. The inputs to this step therefore include the failure conditions from FHA and CCA, system architecture description, description of system equipment, system interfaces with other systems and preliminary CCA (described in Section "Common Cause Analysis (CMA, ZSA, and PRA)") [1].
2. *Determine if the design can be expected to meet identified safety requirements and objectives*
   In this step, each identified severe-major/hazardous and catastrophic failure condition is evaluated in detail. Each of these is analyzed using FTA (discussed in detail below in Section "Fault Tree Analysis") or a similar method to show how item failures either singly or in combination lead to system or at a higher level aircraft failure. This analysis is both qualitative and quantitative. This step demonstrates that all the qualitative and quantitative objectives associated with the failure conditions can be met by the design under consideration. Maintenance intervals for discovery of hidden (latent) failures are also identified in this step. Based on the component systems and their failure consequences identified in the fault trees, the corresponding development assurance level and budgets are developed. All requirements for independence of systems made in the FTA are verified in this step. This step is frequently performed at an early stage in the design, therefore the inputs are based on preliminary domain knowledge, experience with similar designs and judgment available at the time [1].
3. *Derive safety requirements for the design of lower level systems*
   The safety requirements identified at the system level by the preceding steps are then allocated to the items or components making up a system. This involves both hardware and software and is both qualitative and quantitative. It also involves specifications for installation of systems and subsystems (aspects such as segregation, separation of systems, protection from mechanical damage, etc.). Safety allocations include DAL for hardware and software, maintenance intervals and associated "Not to Exceed" times [1].

The PSSA process should be well-documented since this step is frequently revisited during the development process and the reasons for specific design architectures may need to be understood from different perspectives and requirements at different stages of the project.

Fault Tree Analysis

FTA is very powerful, graphical deductive reasoning tool which can identify undesired failure and help the investigator identify their root causes. The technique was developed extensively by the nuclear and aerospace industries and can be

viewed as a systematic method for acquiring information about a system. References [4] and [5] provide a wealth of information about this technique. An introduction to the basic theory of fault trees, including some of the rules of probability theory, Boolean algebra is presented here to introduce the reader to this technique. Medical examples will be presented in Chap. 3.

There are two major methods for performing analysis—inductive and deductive analysis. Inductive analysis involves reasoning from individual cases to a general conclusion [4]. In this method, a particular fault is considered and we attempt to ascertain the effect of that fault or condition on system operation. Examples of this include a fuel pump malfunction and its effects on power output of an engine. Or the effect of failure of an organ and its effect on body function such as renal failure and its consequences on urine output. FMEA, failure modes effects and criticality analysis (FMECA) are some commonly used inductive methods which will be discussed further.

Deductive reasoning method constitutes reasoning from the general to the specific. In this method, we observe that the system has failed in a particular way and we attempt to determine what components failed and in what manner that led to system failure. This is also called "Sherlock Holmesian" thought since the legendary detective had to start with a crime and based on the clues and evidence available reconstruct the events that led to the crime [4]. This mode of analysis is well suited for the investigation of accidents and similar untoward events. FTA is an example of deductive reasoning. Therefore, it lends itself well to medical diagnosis. Inductive reasoning helps tell the investigator what system states can occur, deductive reasoning tells how a particular system state, especially a failure state can occur [4].

A fault tree is a graphical analytic technique composed of the various parallel and sequential combinations of events that will result in the undesired event of system failure. *The method is both qualitative and quantitative*. The undesired event is called the "top event" of a fault tree. Constructing a fault tree requires deep knowledge and insight into the event being investigated since the investigator develops the tree based on knowledge of systems and their connections. The faults can be component hardware failures, software failures, or human failures. *The tree itself represents the logical interrelationships between basic events which can cause the top event of system failure*. It is not an exhaustive enumeration of possibilities, but an exploration of the more likely events which can cause the top event.

The building blocks of a fault tree are primary events, intermediate events, and top events. The building blocks are described here, the symbols are shown in Fig. 2.1. The list is not exhaustive, only the most commonly used events and logic gates are discussed here.

The Primary Events

The primary events of a fault tree are those events which are not further developed. These include the following [4]:

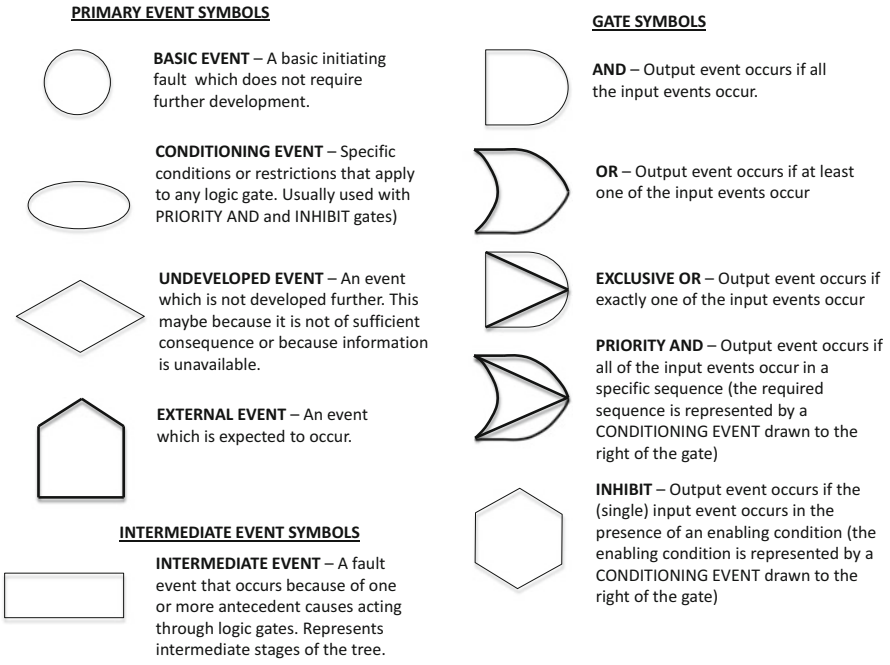

Fig. 2.1 Symbols used in the construction of fault trees, from [4]

1. **Basic event**: This is a basic initiating fault which does not require further development. Examples include fuel valve blocked, microprocessor failure, etc. for top events of engine failure or computer failure. It is represented by a circle.
   (a) **Medical example**: Subtherapeutic INR (basic event) led to thrombus which led to stroke.
2. **Conditioning event**: Specific conditions or restrictions that apply to the logic gates. It is represented by an oval. Used with "Priority AND" and "INHIBIT" gates.
3. **Undeveloped events**: An event which is not developed further, either because developing it further is not relevant for the problem being analyzed or because more information is not available. It is represented by a diamond.
   (a) **Medical example**: A finding uncovered but not relevant to current analysis. Osteoporosis on Chest CT done for lung cancer. Therefore not explored further.
4. **External event**: is an event which is normally expected to occur. For aviation example this includes events such as "icing." These events are not in themselves faults, these events can occur normally. It is represented by the house symbol.

Note that basic events are supposed to be independent in many system safety assumptions which may not be true in the real world.

Intermediate Event Symbols

Intermediate event: a fault event that happens because of one or more primary events acting through logic gates. It is represented by the rectangle symbol.

(a) **Medical example**: Intermediate event: Blood loss (basic event) led to hypotension (Intermediate event) which led to shock liver.

Logic Gates Used in Fault Trees

1. **Boolean "OR" gate**: Output occurs if at least one of the input events occurs.
   (a) **Medical example**: Spinal cord disease OR muscle disease led to weakness.
2. **Boolean "AND" gate**: For this gate, the output occurs if all the inputs are true. The output event occurs if and only if all the input events occur.
   (a) **Medical example**: Right ureter blockage AND left ureter blockage led to kidney failure.
3. **The Inhibit gate**: represented by a hexagon is a special case of the AND gate. The output can be caused by a single input, but a qualifying condition must be present for the output to happen. The conditional input discussed under primary events is the qualifying condition that must be present for the output to happen. Examples include input chemical reagents (input) going to completion (output) in the presence of a catalyst [4].
   (a) **Medical example of Inhibit gate**: (a) Diaphragm weakness from myasthenia gravis in the presence of moderate COPD led to ventilatory failure. Either could not do it alone for a patient with moderate myasthenia gravis and COPD. (b) Stable Congestive Heart Failure (CHF) patient developed hypokalemia (conditioning event) which led to ventricular arrhythmia.

Less frequently used logic gates are the Exclusive OR and Priority AND gates. In an Exclusive OR gate, the output occurs only if one of the inputs occur. When more than one of the inputs happens, the output is zero.

Fault Tree Component Fault Categories

In FTA, faults are classified into three categories—primary, secondary, and command. A primary fault occurs in an environment for which the component is designed. For example, a concrete beam in a building failing under the weight of a load which is less than what the beam is designed for. A secondary failure is a component or system failure in an environment which it is not designed for [4]. For the example above, this

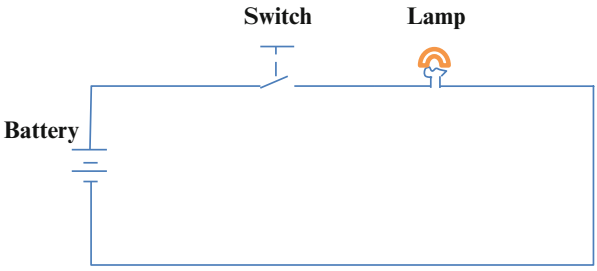

Fig. 2.2 Simple system to illustrate failure effects, modes, and mechanisms. The battery provides the energy for operation of a lamp controlled through a switch

Table 2.1 Failure modes, effects, and mechanisms involved for the example of Fig. 2.2

Failure effect	Failure mode	Mechanism
Switch fails	– Contacts broken	– Mechanical damage
	– High-contact resistance	– Corrosion of contacts
Lamp fails to light	– Lamp filament broken	– Material defect, excess voltage
	– Lamp glass broken	– Mechanical shock
	– Loose contact with socket	– Human error, socket defects
	– Socket contacts damaged	– Human error, socket defects
Low voltage from battery	– Leakage of electrolyte	– Defective casing
	– Contacts broken	– Mechanical shock
Open circuit	– Wire broken	– Mechanical shock, human error
	– Wire burnt	– Short circuit, excessive current

involves the beam failing under a weight more than what it was designed for [4]. A command failure is the proper operation of a component at the wrong time or place.

Failure effects, failure modes, and failure mechanisms are important concepts in analyzing the relationships between events. Consider Fig. 2.2 which shows a simple circuit controlling operation of a lamp based on an illustrative example in [4].

Failure effects understands failures based on their importance—what are the consequences or effects of failure on the system [4]. Failure modes helps describe the specific manner in which failure occurs. Failure mechanisms helps identify the cause(s) of the failure modes [4]. For the example of Fig. 2.2, this is shown in Table 2.1. For example, the failure effect of low voltage from battery can occur due to the failure mode of leakage of electrolyte from battery. Defects in casing of the battery or mechanical shock are the failure mechanisms which can cause leakage of electrolyte from battery.

Lamp System Failure Analysis

The middle column, "system failure modes" constitutes the "top event" that the system analyst has to explore. In fault tree methodology, one of these is selected and the immediate preceding causes of this in column 3 are explored. These immediate

causes will constitute the top events for the subsystem being examined which will then be used to extend the analysis to the chosen subsystems to form the next layer of the fault tree [4]. Consider the toy example of left middle cerebral artery occlusion leading to ischemic stroke. For this example, failure effect is global aphasia (a failure effect which will be classified as severe), failure mode is thrombotic occlusion of the left middle cerebral artery. Failure mechanism could be left carotid atherosclerosis, cardiac embolism, traumatic dissection, vasculitis, and other rare causes of stroke. Working backwards from failure modes to failure mechanisms allows for rigorous examination of the causes of thrombotic stroke.

The system analyst first defines his system and establishes boundaries. He then selects a particular system failure mode as the "*top event*" for further analysis. The system analyst then determines the "immediate, necessary, and sufficient" causes for the occurrence of this top event. These are not the basic causes, but the immediate causes of mechanisms of this event. Once the immediate, necessary, and sufficient causes of the global top event are determined, these in turn are considered the subtop events and the analyst proceeds onto determine the immediate, necessary, and sufficient causes of these. The analysis proceeds by switching back and forth between failure mechanisms and failure modes i.e., the "mechanism" for a system are the modes for the subsystem. Thinking in immediate, *necessary, and sufficient steps is an extremely important principle called the* "*Think Small*" *rule. This proceeds till the desired limit of resolution is reached* [4].

The construction of fault trees follows some basic rules [1, 4, 5]. These are:

1. *State the undesired top level event in a clear, concise statement*. This should be clarified precisely as to what it is and when it occurs.
2. *Develop the upper and intermediate tiers of the fault tree*; determine the intermediate failures and combinations which are immediate, necessary, and sufficient to cause the top level events and interconnect them by the appropriate logic symbols [1, 4]. Extend each fault event to the next lower level. At each level of tree construction, particular attention is paid to the following:
   - Can any single failures cause the event to happen?
   - Are multiple failure combinations necessary for the event to happen?
3. *Develop each fault tree event through more detailed levels of system design till the limit of resolution is reached and a root cause*(*s*) *is established*. Root cause analysis is explored further as a management method in Chap. 8.
4. Evaluate the fault tree in qualitative and/or quantitative terms. Fault trees are qualitative by nature of their construction. Establish probability of failure for individual components; evaluate ability of the system to meet safety margins. If safety objectives are unmet, redesign the system and reiterate the process.

Two other procedural rules are complete the Gate rule and No-Gate-to-Gate rule. The complete the Gate rule states that all inputs to a particular gate should be completely defined before further analysis of any of the inputs is undertaken. The No-Gate-to-Gate rule states that gate inputs should be well defined gate events and the outputs of individual gates should not be connected to other gates. *Once the root*

cause(s) are identified, the investigator must be able to reconstruct the top event by traversing up the tree. As discussed in the appendices, the idea behind the analysis is to identify the "minimal cut set." A "minimal cut set is the smallest combination of component failures, which, if they occur will cause the top event to happen" [1]. It follows by logical extension (see appendices for details) that if a single system failure can cause the top event to happen, then the design is not a fault tolerant system. It also helps understand why there is protection in redundancy (assuming independent failures). Consider a design made of two systems A and B, each with probability of failure of 1/1,000. Let us assume that our first design can fail if system A OR system B fails. Therefore, the probability of the undesired top event happening remains of the order of 1/1,000. Now let us assume systems A and B are used in a redundant manner and both must fail for the undesired top event to occur. Now the probability of failure becomes 1/1,000 × 1/1,000 or 1 in 1,000,000.

Basic ideas from probability are discussed in the following section. Appendices 1 and 2 contain further information on FTA and a closely related structure called DD, their construction and analysis using probability theory and Boolean algebra. The information in the appendices is useful for more mathematically inclined readers and can be safely skipped for understanding the use of FTA methodology for medical diagnosis used in the rest of this book.

Probability Basics

We explore some basic probability theory which has ubiquitous application in decision making. This section looks at a few basic rules from probability theory necessary for understanding fault trees and analyzing them. $P(\mathrm{A})$ is a real number between 0 and 1 which denotes the probability of event A happening. Similarly $P(\mathrm{B})$ is the probability of event B happening. A number closer to 1 denotes a higher probability; numbers closer to 0 denote low probabilities. $P(\mathrm{A}\cup\mathrm{B})$ is the probability of event A or event B happening. $P(\mathrm{A}\cap\mathrm{B})$ is the joint probability of events A and B happening [6].

1. $P(\mathrm{A}\cup\mathrm{B}) = P(\mathrm{A}) + P(\mathrm{B}) - P(\mathrm{A}\cap\mathrm{B})$. This operation happens at the OR gate of the fault tree.
2. $P(\mathrm{A}\cap\mathrm{B}) = P(\mathrm{A}) \cdot P(\mathrm{B}|\mathrm{A})$. This operation happens at the AND gate of the fault tree.

$P(\mathrm{B}|\mathrm{A})$ denotes the probability of event B happening provided we know A has happened. For example, assume a box has ten pairs of socks, of which five pairs are white, three are red, and two are blue. The collection of all socks: white, blue, and red is called the universal set which denotes all possible outcomes. $P(\text{white socks}) = 5/10$, $P(\text{red socks}) = 3/10$ and $P(\text{blue socks}) = 2/10$. However, if we know that a colored sock was drawn from the box, we have restricted our possibilities to 5 since there are three red and two blue socks in the box which are colored. If we have this information, then the probability that a drawn pair of socks is red is

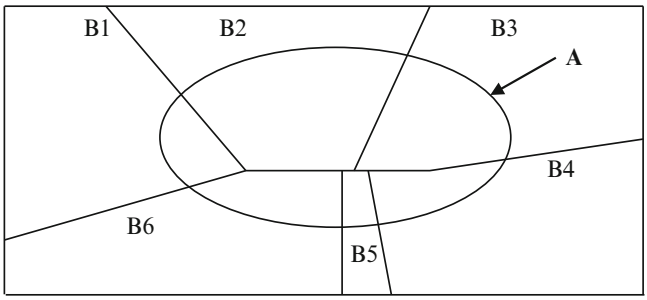

Fig. 2.3 Bayes theorem. The *rectangle* represents the universal set—all possible events. It is partitioned into different regions. Given the occurrence of event A, we are interested in knowing the probability that it originated from a particular region. In the context of reliability, let B1, B2, . . . , B6 represent six different manufacturers of a particular component. Let A represent all defective components. If we have a particular defective component, what is the probability that it was manufactured by manufacturer B1? Bayes analysis helps estimate such probabilities [4]

P(Red Socks|Colored Socks) = 3/5. Similarly P(Blue Socks|Colored Socks) = 2/5 instead of 3/10 or 2/10 if we did not have this information.

If A and B are independent events, where the occurrence of one does not influence the occurrence of the other, $P(\mathrm{A} \cap \mathrm{B}) = P(\mathrm{A}) \cdot P(\mathrm{B})$. An important probabilistic method is Bayes theorem where we are interested in calculating the posterior probabilities of an event. This is a powerful method which forms the heart of many algorithms in artificial intelligence and machine learning [6].

Let the universal set (rectangle in Fig. 2.3) be partitioned into six different regions. B1 + B2. . .B6 = Universal set. Let this be denoted by Bi where i assumes values between 1 and 6 to denote each of the six regions. There is no overlap between the partitions. For the example above, this can be expressed as:

$$\Omega = \sum_{i=1}^{6} \mathrm{B}i \tag{2.1}$$

(In Eq. (2.1) the symbol $\sum$ denotes addition i.e., B1 + B2 + B3 + B4 + B5 + B6.)

The event A can occur as part of the partitions of the universal set as the different regions of overlap of A and individual Bi's demonstrate. We are interested in finding a particular Bi, given the event A has happened [4]. This can be done using Bayes rule:

$$P\left(\mathrm{B}i \middle| \mathrm{A}\right) = \frac{P(\mathrm{B}i \cap \mathrm{A})}{P(\mathrm{A})} \tag{2.2}$$

The event A can occur as part of many different partitions of the universal set. In the example in Fig. 2.3, the total probability of a defective component is the sum of individual probabilities of defectives made by different manufacturers. Therefore

$P(\mathrm{A}) = \sum_{i=1}^{6} P(\mathrm{B}i)P(\mathrm{A}|\mathrm{B}i)$. Assume we are interested in knowing $P(\mathrm{B2|A})$ or in other words the probability of a defective part made by manufacturer # 2. This is called the posterior probability [4]. Substituting the relevant terms, the corresponding posterior probability becomes:

$$P(\mathrm{B2}|\mathrm{A}) = \frac{P(\mathrm{A}|\mathrm{B2})P(\mathrm{B2})}{\sum_{i=1}^{6} P(\mathrm{B}i)P(\mathrm{A}|\mathrm{B}i)} \tag{2.3}$$

Toy Medical Example

To illustrate medical application of Bayes rule, consider the following example. Let the universal set be the set of patients with the following conditions: B1: CHF, B2: COPD (chronic bronchitis and emphysema), B3: Bronchial Asthma, B4: Pulmonary Embolism, B5: myasthenia gravis, and B6: Muscular Dystrophies. Let the region A denote the patients within this universal set who are short of breath. We are interested in knowing what is the probability that a patient with shortness of breath has a particular diagnosis—such as myasthenia gravis.

To make the example illustrative, let the numbers be as follows:

Total number of patients, the universal set: 100.

B1: CHF patients: 30. 30 % of whom are short of breath: 9 patients. Therefore, probability of shortness of breath given that the patient has CHF is given by $P(\mathrm{A|B1}) = 0.3$. $P(\mathrm{B1}) = 30/100 = 0.3$

B2: COPD patients: 30. 50 % of whom are short of breath: 15 patients. Therefore $P(\mathrm{A|B2}) = 0.5$.
$P(\mathrm{B2}) = 30/100 = 0.3$

B3: Bronchial Asthma patients: 20. 20 % of whom are short of breath: 4 patients. Therefore $P(\mathrm{A|B3}) = 0.2$. $P(\mathrm{B3}) = 0.2$

B4: Pulmonary Embolism: 5 patients. 60 % of whom are short of breath: 3 patients. Therefore $P(\mathrm{A|B4}) = 0.6$. $P(\mathrm{B4}) = 0.05$

B5: Myasthenia gravis: 5 patients. 80 % of whom are short of breath: 4 patients. Therefore $P(\mathrm{A|B5}) = 0.80$. $P(\mathrm{B5}) = 0.05$

B6: Muscular Dystrophy: 10 patients. 40 % of whom are short of breath: 4 patients. Therefore $P(\mathrm{A|B6}) = 0.40$. $P(\mathrm{B6}) = 0.1$

We are interested in determining what is the probability of myasthenia gravis given that a patient is short of breath. In other words, we would like to know $P(\mathrm{B5|A})$? By application of Bayes rule from Eq. (2.3):

$$P(\mathrm{B5}|\mathrm{A}) = \frac{P(\mathrm{A}|\mathrm{B5})P(\mathrm{B5})}{\sum_{i=1}^{6} P(\mathrm{B}i)P(\mathrm{A}|\mathrm{B}i)}$$

$$= \frac{(0.80) \times (0.05)}{0.3 \times 0.3 + 0.3 \times 0.5 + 0.2 \times 0.2 + 0.6 \times 0.05 + 0.80 \times 0.05 + 0.4 \times 0.1}$$

$$= \frac{0.04}{0.39} = 0.102 \text{ or approximately } 10\ \%$$

This shows that even though most patients with myasthenia gravis are short of breath (as high as 80 % in the above hypothetical example), since myasthenia is a rare disease in the population when compared with more common causes like COPD and CHF in this example, the overall posterior probability that a patient with shortness of breath has myasthenia gravis is low.

Failure Modes and Effect Analysis

FMEA is a powerful inductive analysis method. FMEA is a method of identifying the failure modes of a system or a piece-part and determining the effects on the next higher level of design [1]. It can be performed at any level within the system (function, black box, piece-part, etc.) [1]. An FMEA can be qualitative or quantitative. FMEA plays an important role in systems safety analysis and supports deductive techniques such as FTA, DD, or MA. FMEA is performed at a given level by analyzing the different ways in which a system may fail. The effect of each failure mode at a given level and the next higher level is determined. FMEA provides answers to the "*What happens if*?" question [4]. The process involves assuming a certain state of function of a component or system, determining the different manners in which it can fail and determining the effect of that component on the rest of the system. The method is illustrated through the example in Fig. 2.4 [1, 4].

The power supply system can fail in many different ways with varying degrees of impact on the system to provide electrical power to the motor. Assume that the generator is the primary power supply with the battery being the backup. A switching mechanism can switch between the generator and backup battery if the generator fails. The battery can provide limited power (for a few hours) till the generator can be restored online. Table 2.2 shows the failure modes of this system.

Table 2.2 lists the components, failure modes of each component, individual probabilities of those happening, and effects on electric motor functioning—classified as minor (motor functions at reasonable but suboptimal level), major (decreased safety margin or motor power output at less than 50 %), severe (severely decreased safety margin or motor output less than 20 %), and critical (motor is completely unable to function). If the switching mechanism fails due to contacts being broken, then the motor fails in a critical manner since power supply to it is completely

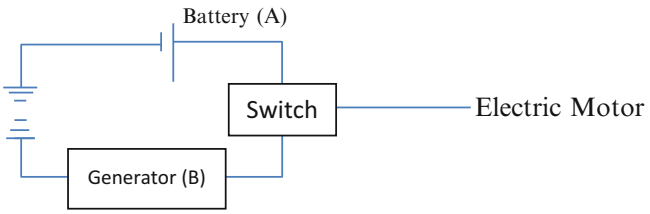

Fig. 2.4 A diesel generator (B) or battery provides electric power for operating a motor selected through a switch. The failure modes of the system are as shown in Table 2.2

Table 2.2 FMEA of power supply system in Fig. 2.4

Component	Failure mode	Probability	Effects on motor
Battery	Low voltage	1×10^{-3}	Major
	Short circuit	1×10^{-6}	Critical
	Fluctuating voltage	1×10^{-2}	Minor
Diesel generator	Engine failure	1×10^{-4}	Severe
	Alternator failure	1×10^{-8}	Severe
	Fluctuating voltage	1×10^{-2}	Minor
Switch	Stuck in generator	1×10^{-6}	Major
	Contacts broken	5×10^{-3}	Critical

disrupted. If it fails in generator mode, the system loses redundancy completely and is unable to switch to battery mode if the generator fails for any reason. In this situation, as long as the generator works, the electric motor continues to work. This failure decreases the safety margin of the system and is therefore classified as major. The moment the generator fails, the electric motor stops since it is unable to switch. This is therefore a latent failure which is classified for this example as a major failure but is not critical. It also has a low probability—1×10^{-6} of occurrence. If the engine of the generator or its alternator fails, the effect on the system is severe since the backup power source—the battery has a capability of providing function only for a few hours. Similarly if the battery fails in short circuit mode and is the sole power source when the generator is down, it causes critical failure. If it fails in low voltage mode, it can cause major effects on motor functioning, but some function would still be provided. Fluctuating voltage can cause fluctuations in motor performance but without failure of service or motor damage, therefore it is classified as minor.

Table 2.2 provides invaluable information on the failure modes and helps identify the components and the respective failure modes with "critical" and "noncritical" effects. The table can be expanded to include numerous other failure modes of the system including "vibration," "engine overheating" with their respective effects on the motor and other interacting systems. In the example above, vibration may cause a slight increase in wear and tear; therefore its effect might be classified as mild. Overheating of the engine compartment may be classified as "major." The quantitative probability information provided by this table can be used for assessing failure probabilities—for example assuming independent failures, the system has a

$5 \times 10^{-3} + 1 \times 10^{-6}$ risk of critical failure. This can be approximated to 5×10^{-3} since the contribution of the 10^{-6} term is negligible. Adding up the failure modes listed as "Severe," we see that the corresponding probability is $1 \times 10^{-4} + 1 \times 10^{-8}$ (engine failure, alternator failure) which can be approximated to 1×10^{-4} (or 1 in 10,000) since the contribution of the other term is negligible.

Analyzing this system, we see that the probability of critical failure is too high, in other words there is a 5 in 1,000 chance of the system failing due to the switch's contacts being broken so that the motor will not work. The net result of the FMEA is it helps allocate resources appropriately. Designers therefore need to invest research and development into designing a better switch with a lower failure probability rate, especially one which will not fail in contacts broken mode. Investments for protecting against fluctuating battery voltage do not make the system safer since their effect on the electric motor is "minor" and the estimated probability of occurrence is also low.

Based on the above toy example, we can now look at the more formal methods for performing an FMEA [1]. The three major steps involved in FMEA are preparation, analysis, and documentation [1].

FMEA Preparation

The first step towards performing a FMEA is determining the customer's requirements, obtaining system documentation, and understanding the operation of the system [1]. The analyst obtains safety-related information, data on failure rates, and information on different failure modes. Functional drawings of the systems of interest, knowledge of probability of failure rates, data from prior experience with similar systems are important. It is important to identify the failure detection mechanism for each component since in many systems it can be latent [1]. Failure detection methods include error monitors, self-test algorithms, and periodic maintenance checks [1].

FMEA Analysis

It is important to determine the objectives and level of resolution of the FMEA. One method which is helpful is to divide the system into functional blocks. Once this is achieved, for each functional block, internal functions and interactions with all connected systems should be analyzed carefully. The next step is to postulate failure modes for each functional block. This requires great insight into the functional block being studied to ask the "*what if*?" questions. Failure effects should be classified based on severity and damage potential with attention dedicated to the most critical. For the example in Fig. 2.4 and Table 2.2, failure of the switch in contacts broken mode is the most critical weakness in the system. Other failure modes with less impact on functionality are explored progressively—those

classified as severe, major, minor, and so on. For each failure mode and failure effect category, the analyst considers the method of failure detection [1]. It is important for the analyst to document his thought process, the assumptions being made, the justification for each failure mode, justification behind the assigned failure rates and rationale for assigning a failure mode to the particular failure effect category. Maintaining the necessary documentation explaining the analysis is very important for later review or independent verification. Quantitative analysis can then be performed from available reliability data based on past experience. The above is applicable for analyzing the effect of the failure mode on the functional block itself and on the next higher level of function.

The next level of resolution in performing an FMEA is to look at each individual component of a functional block called piece-part FMEA. The first step in this process is to create a list of all components (parts list) to be analyzed, followed by their respective failure modes [1]. This can be a challenging task for complex components like integrated circuits consisting of thousands of individual components. Further steps in a piece-part FMEA proceed similar to the functional FMEA, including assessing the impact of failure on the next higher level of function, methods involved in fault detection, and documenting assumptions and rationale behind and analysis. In general, all possible ways that the component can fail to perform its functions must be considered for inclusion in the list of component failure modes. There are certain failure modes which are common across a diverse array of components and must be considered. These include short and open circuit, inoperative mode, intermittent operation, false settings, miscalibration, mechanical wear and tear, loose contacts or loose assembly and fracture, etc. For complex digital devices, computer simulations of different components needs to be performed [1].

FMEA Documentation

The capstone of FMEA preparation and analysis is the FMEA documentation. The recommended report for an FMEA includes [1]:

1. An introductory statement containing a statement about the purpose and objective of the FMEA.
2. Description of how the analysis was performed—listing of assumptions made, description of the analytic methods used, software simulations performed, and limitations of the FMEA.
3. A complete listing of results of the FMEA, including component identification. This is performed in a tabular form as shown in Tables 2.1 and 2.2.
4. Appendices that include drawings or schematic diagrams, any failure mode distributions for lower level components defined during analysis [1].
5. A list of failure rates and their sources used for performing the FMEA.

A related topic is FMECA. In this analysis, criticality of the failure is analyzed in greater detail and controls or mitigating systems are described for limiting the

likelihood of such failures. It is frequently used as a part of SSA. The four aspects of this approach are: (1) fault identification (identifies the possible hazardous condition), (2) effects of fault (explains why this is a problem), (3) projected compensation or control (what has been done to mitigate the effect of failure and control the condition), and (4) summary of findings (whether the situation being analyzed is mitigated or whether further steps should be taken) [4].

One of the most important aspects to realize is that FMEA is a qualitative technique. Therefore it requires great domain expertise and insight. For highly complex systems involving multiple functional blocks (software, engineering, mechanical system, etc.), it is very difficult for a single analyst to possess adequate domain expertise across the spectrum of disciplines involved in the FMEA. In these circumstances, it is very important for a team approach where each set of experts analyzes their relevant systems with excellent interdisciplinary understanding and collaboration between teams to synergize the FMEA [4].

Fault Hazard Analysis (FHA) is a related extension of FMEA which is useful for projects spanning different organizations with one acting as the integrator. This technique is useful for detecting faults that cross organizational interfaces. A typical FHA involves the following columns, the first five of which are used in FMEA [4].

Column 1: Component identification
Column 2: Failure probability
Column 3: Failure modes. (Identify all possible failure modes)
Column 4: Percent failures by mode
Column 5: Effects of failure
Column 6: Identification of upstream component that could initiate the fault being analyzed
Column 7: Factors that could contribute to secondary failures
Column 8: Remarks

Failure modes and effects summary (FMES) is a grouping of single failure modes which produce the same effect [1]. For the toy example in Fig. 2.4, engine failure, alternator failure both cause severe failure effects on electric motor function and would be classified similarly. FMEA is a very powerful tool which helps with treatment planning. While this chapter provides a systematic introduction to the theory of FMEA, medical case examples encountered in clinic will be presented in a subsequent chapter.

Common Cause Analysis (CMA, ZSA, and PRA)

CCA which refers to CMA, ZSA, and PRA is discussed briefly here. These methods look for the numerous common causes which can frustrate the assumption of independence between system failures thereby compromising system safety [1].

Common Mode Analysis

CMA is a qualitative analysis tool used to evaluate a design, especially to understand the integration of component systems. It can be carried out at all levels of design. They are performed to verify that logical AND events in a fault tree are truly independent. Errors in design, manufacturing, maintenance, installation of system components which can defeat safety in redundancy should be carefully analyzed [1]. For example, components with identical hardware and/or software are susceptible to generic faults which could cause abnormalities in multiple systems [1]. For example, suppose systems A AND B need to fail for the top event to happen. Suppose a component of both systems is made by the same manufacturer with a software design error which can cause critical loss of function of both systems under certain circumstances. This creates a common vulnerability in both systems; therefore the assumption of independent failures of systems A and B is no longer valid. A common cause can trigger a simultaneous critical failure of both systems frustrating redundancy in design. When performing CMA, wherever required redundancy is compromised, the analyst must justify the rationale for accepting or rejecting the compromise [1]. The following common mode errors are considered in most analysis [1]: software development errors, hardware development errors, manufacturing/installation/maintenance errors, environmental factors (temperature, vibration, humidity, etc.), calibration errors, etc. [1].

Similar to FMEA, the method is qualitative, often interdisciplinary requiring expertise across multiple domains. The analyst therefore needs to understand the system from design to installation and preventive maintenance [1]. This includes knowledge of design, equipment and component characteristics, maintenance and testing tasks, installation crew practices and procedures, and system specifications (software and hardware). The analysis is performed by examining common susceptibilities from the viewpoint of the common safeguards employed to minimize the risks of common mode faults. These include diversity and dissimilarity in design and manufacturing, testing and preventive maintenance, design quality levels, and training of personnel [1].

The analysis itself proceeds along the following ways: For each hazardous event or catastrophic event in FHA and PSSA, the analyst evaluates each AND event in the FTA (or dependence diagram—see appendices) and verifies the independence principle hold true. The analyst then documents that CMA requirements have been satisfied. A subsequent analysis evaluates CMA events not derivable from FTA/DD methods such as generic failures, environmental effects, physical installation, etc. [1]. Once common mode vulnerabilities are identified, solutions are proposed and design changes are implemented. The entire FTA/DD/CMA process is then iterated till the final design is finalized. The documentation proceeds in a manner similar to FMEA.

Zonal Safety Analysis

ZSA examines physical installation considerations of system hardware which can impair independence between systems. For example, if two critical computer systems A and B are placed in close physical proximity to one another, then an event such as computer A catching fire can cause failure of computer B by their close physical proximity. ZSA examines the influence of physical proximity of such systems which can weaken independence between system failures. In the design of products, especially complex systems such as aircraft, ZSA should be performed early in the design before structural modifications will need to be made at an advanced stage in product development. The conclusions of ZSA will provide inputs to the SSA. Commercial fly-by wire airplanes mitigate this risk by placing computer systems in different areas of the plane so that a limited fire or explosion will not disable all vital systems. Further details can be found in [1].

Medical Example

ZSA examples abound in medicine. The following are frequently encountered and to a great extent preventable. Examples include pneumothorax from subclavian central line placement, brachial plexus injury from stretching during surgical positioning leading to upper extremity weakness; sciatic nerve injury from hip surgery, peroneal nerve injury from knee surgery, and femoral nerve injury during pelvic procedures. Performing ZSA can help prevent and mitigate these from happening and once they happen, channel investigation and treatment in the right direction.

Particular Risks Analysis

This refers to those events which while being outside of the systems and components being analyzed will violate failure independence of systems and cause system failure. This includes events such as fire, hail, lightning strikes, radiation, explosions, etc. Each such identified risk should be the subject of a study examining the cascade of effects associated with the event. Please see [1] for further details. *Medical examples*: Common medical examples include Raynaud's phenomenon and cold exposure, worsening of myasthenia gravis in the summer and with intercurrent infection such as the flu.

Case Example

L.H. is a 69 y/o female with ocular myasthenia gravis. Since symptoms remained isolated to the eyes for over 3 years, the risk of systemic involvement was considered

low. Patient was treated with low-dose Prednisone monotherapy ranging between 5 and 7.5 mg/day. Symptoms remained stable for 2 years before a bad seasonal flu triggered considerable worsening of ptosis, diplopia, and morbidity from ocular myasthenia gravis. The worsening of symptoms due to seasonal flu required over 6 weeks of moderate dose prednisone ranging from 20 to 30 mg to treat.

The main challenge in CCA is to define the analysis perimeter [7]. The data guiding this analysis originates from practical in-service experience and are transformed in envelope cases by aviation safety agencies. CCA has an enormous impact on structural architecture, therefore it must be performed at an early stage in the design to avoid extremely expensive late design changes.

These methods of analysis integrate into the *system safety assessment or SSA*. An SSA is a systematic, thorough evaluation of the implemented system to demonstrate that safety requirements are all met [1]. As discussed earlier, the difference between the PSSA and SSA is that while PSSA is a method to evaluate the proposed design or architecture and derive safety requirements, the SSA is verification that the implemented design meets both qualitative and quantitative requirements as defined in the FHA and PSSA [1]. The SSA integrates all the analysis (FTA/DD, FMEA, FMECA, CMA, ZSA, and PRA) described above qualitatively and quantitatively to verify the safety of the overall system and cover all the safety concerns identified in the PSSA. Therefore, typically this includes the following information [1]:

- System description
- Failure conditions (FHA, PSSA)
- Failure condition classification (FHA, PSSA)
- Qualitative analysis for failure conditions (FTA, DD, FMES)
- Quantitative analysis of failure conditions (FTA, DD, MA, FMES, etc.)
- Common cause analysis
- Safety-related tasks and their intervals (FTA, DD, FMES, MA)
- DAL for hardware and software (PSSA)
- Verification that safety requirements from the PSSA are incorporated into design and/or testing
- The results of nonanalytic verification process (test, demonstration, inspection)

The above sections provide a tutorial overview of the rigorous safety techniques involved in safety borrowed from the aerospace and nuclear industries. The methods discussed can be adapted based on requirements and have broad application. These can be applied to the successful operation of a coffee shop, designing an automobile or to healthcare. It is extremely important to realize that safety is analyzed from both micro and macro perspectives, not only should the individual ball bearing in an aircraft landing gear be analyzed but its ripple effect on higher systems has to be simulated and predicted as well [7].

Case Example: SSA of Pulse IV Methylprednisolone Treatment

Immunosuppression is an unfortunate but necessary part of the practice of neuromuscular medicine. There are numerous methods for performing immunosuppression, oral daily prednisone has been the most widely used and traditional method for the treatment of a variety of diseases in autoimmune neurology and rheumatology. Daily prednisone has a plethora of side effects and for diseases with very long time courses such as CIDP where a high dose maybe necessary over months, they may seem unacceptable. Based on a review of the literature, an attempt was made to switch from daily oral prednisone to pulse IV Methylprednisolone where a high dose of methylprednisolone (between 500 and 1,000 mg) is given IV every few weeks without daily oral steroids [8]. Before instituting this practice, an SSA was conducted. The basis for the SSA was literature review detailing past safety-related side effects from the published literature [8, 9], prior personal and institutional experience. The following major considerations were identified: drug administration syndrome consisting of insomnia, heartburn, sweating, flushing, erythema; weight gain, cushingoid features; glucose intolerance/steroid induced diabetes mellitus, muscle cramps, joint pains, and hypertension [8, 9]. Other listed side effects including lymphoma are rare and not included in the current analysis since this is meant for initial proof of principle. Considering IV Methylprednisolone as a system, the following analysis was used:

1. **Function definition**: IV Methylprednisolone for treatment of inflammatory neuropathy.
2. **Functional hazard assessment** (**FHA**):

   2A. Loss of effective immunosuppression. (Drug being ineffective)
   2B. Major adverse side effects

3. **FTA of failure conditions identified in FHA**: In this step, we will construct fault trees for each functional failure condition identified in (2)

   3.1: **FTA for failure condition 2A**

      3.1.1. **Top event**: Loss of effective immunosuppression.
      3.1.2. *Immediate*, *necessary*, *sufficient causes* for loss of effective immunosuppression include: drug intrinsically ineffective for the condition OR inadequate intensity of current regimen.
      3.1.3. Expanding the tree further: drug intrinsically ineffective for the condition is a basic event and will not be explored further.
      3.1.4. Expanding inadequate intensity of current regimen further, this can happen if dose administered is too low OR the dosing frequency is too infrequent. Further corrective action can be planned based on which of these is the major consideration.

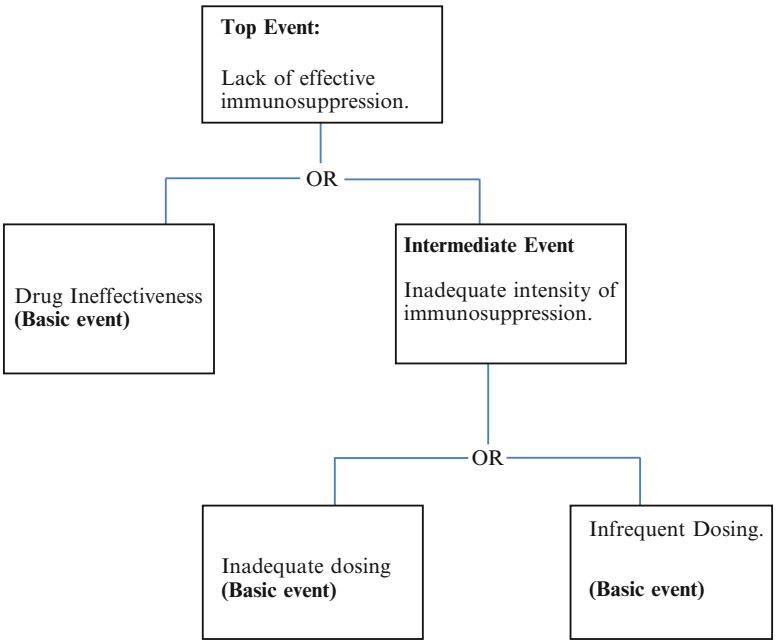

Fig. 2.5 FTA for the top event of lack of effective immunosuppression with IV Methylprednisolone therapy for planned treatment of CIDP

The FTA for the above analysis is shown in Fig. 2.5. For the sake of simplicity, *these trees are constructed with the logical operators inserted in English instead of their mathematical symbols*.

3.2: **FMEA for Lack of Therapeutic Efficiency**: Based on this FHA and FTA, failure modes in terms of therapeutic failure can be identified with relevant consequences and severity classification and mitigation. For the case of CIDP, where there is malfunction of nerves, the following failure modes require consideration. *A*: *Loss of sensory function leading to numbness*, *loss of proprioception*: Numbness by itself is disturbing and can lead to inadvertent physical injury. Based on past experience with similar conditions in related patient populations (example: inherited neuropathies such as Charcot Marie Tooth where there is numbness without pain), patients adapt well to it without safety ramifications. Therefore this is a failure mode with minor ramifications. *B*: *Abnormal sensory function with consequent pain*, *paresthesias*: This failure mode is the most perceived and the most distressing to patients, greatly affecting quality of life. However, this has very limited safety effect and to varying extents can be managed with analgesic medications with wide safety margins, low costs despite the underlying disease itself being poorly controlled. Therefore this is classified as minor, despite being the most obvious manifestation of treatment failure

C: *Loss of motor function in upper extremities*: This can adversely impair all aspects of life—such as eating, reading, and lead to the need for continuous supportive care. Therefore this is classified as major. *D*: *Loss of motor function in lower extremities*: This is another obvious source of morbidity and further injury from falls. *D1*: *Loss of mobility due to lack of strength* where the legs buckle when the patient attempts to stand. Therefore this failure mode is effective only when patient is standing and does not impair sitting and lying down. *D2*: *Loss of mobility due to loss of lack of proprioception* (*lack of balance*): in this mode, a patient has the strength to stand and support his weight, but given lack of knowledge of where the feet are, there is a tendency to fall easily. To some extent, patients compensate with vision to know where their feet are and a cane or walker can help secure balance and prevent falls. Therefore, this failure mode is most limiting in poor light, uneven ground and not operative when sitting and less restrictive on even floors. This failure mode originates in the sensory system but manifests in impairing motor function.

Since progression of motor failure can lead to irreversible loss of function, the discovery of motor failure mode should trigger immediate corrective action in terms of aggressive immunosuppressive therapy.

Based on this, the following FMEA report can be constructed. As described earlier, the following aspects are included in the FMEA documentation.

(a) **Introductory statement** containing a statement about the purpose and objective of the FMEA: The objective of this FMEA is to describe the failure conditions, failure severity, exacerbating conditions, and mitigation strategies associated with failure of treatment with IV Methylprednisolone therapy.

(b) **Description of how the analysis was performed**: This analysis was performed based on a review of the literature detailing the experience of other investigators with the use of IV Methylprednisolone [8, 9] for CIDP and other autoimmune diseases. Failure modes from prior experience with similar conditions such as Charcot Marie Tooth, diabetic neuropathy, and idiopathic neuropathies were also incorporated into the analysis based on assumed similarities.

Assumptions: (1) The treatment trial will be limited, therefore only clinical concerns relevant to a time frame of 8–12 weeks of treatment are being considered.

Limitations of the FMEA include lack of rigorous quantitative data due to limited prior experience; limiting analysis to more immediate and frequently encountered failure modes and not incorporating long-term consequences of immunosuppression such as malignancy.

Table 2.3 FMEA report for loss of therapeutic efficiency of IV Methylprednisolone therapy for CIDP

Function name	Failure mode	Failure environment (lying, sitting, standing)	Failure severity	Mitigation strategies	Comments
Sensory function	Numbness	All phases	Minor	Avoid hot, sharp surfaces, frequent examination of hands, legs, feet	Patient education for mitigating injuries
Sensory function/ motor function	Loss of proprioception	Standing, walking on uneven ground, evening and night. Unsafe driving	*Major*	Avoid uneven surfaces, poor light. Cane, walker for improved balance. Gait Training	Emphasize and develop adaptation strategies
Sensory function	Pain, paresthesias: burning, cold, electric shocks	Resting, lying down. Sometimes better with ambulation	Minor	*Initial and mild pain*: Gabapentin, Pregabalin, Duloxetine, Nortriptyline. *Moderate pain*: Tramadol. *Severe pain*: Opioids	Consider drug combinations. Consider increasing immunosuppression
Motor function	Loss of function in hands	All phases	*Major/ hazardous*	Occupational therapy, Nursing Home, Home health aides	*Increase immunosuppression*
Motor function	Loss of strength and function in legs	Weight bearing phase, standing, walking	*Major*	Physical therapy, occupational therapy	*Increase immunosuppression*

As seen in column 4, the PSSA process shows three failure modes with major consequences and two with minor consequences

(c) **A complete listing of results of the FMEA**: Detailed in Table 2.3.
(d) **Appendices**: Expanded list of side effects, including those not analyzed in this FMEA associated with pulse methylprednisolone therapy are listed in the appendices [8, 9]. (Not shown for this example.)

FMEA header information: see 3.2a, 3.2b, 3.2c, and 3.2.d.

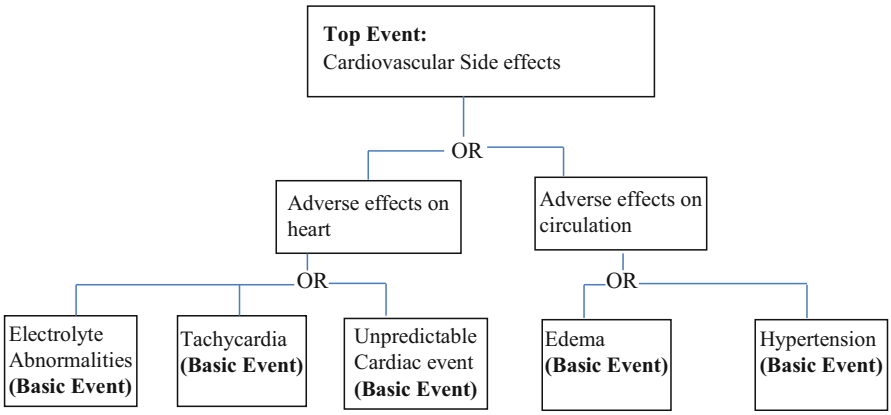

Fig. 2.6 FTA for the top event of cardiac side effects with IV Methylprednisolone therapy for planned treatment of CIDP

3.3. **FTA for failure condition 2B**: An FTA needs to be constructed for each major adverse effect. Cardiovascular and endocrine (blood glucose) adverse effects are explored here since these are the major anticipated adverse effects expected in the short term.

3.3.1. **Top event**: Cardiovascular adverse effects
3.3.2. **Immediate**, **necessary**, **sufficient** causes of the top event include: adverse effects on heart OR adverse effects on circulation.
3.3.3. **Expanding**: adverse effects on heart include tachycardia OR electrolyte changes OR unpredictable effects. Adverse effects on circulation include edema from salt and water retention OR hypertension. These will not be explored further since this is the desired depth of resolution of the fault tree.

The corresponding fault tree is shown in Fig. 2.6.

3.4. FTA for adverse effects on blood glucose.

3.4.1. **Top event**: Blood glucose abnormalities
3.4.2. **Immediate**, **necessary**, **sufficient** causes of the top event include: impaired glucose tolerance OR development of diabetes mellitus.
3.4.3. **Expanding**: impaired glucose tolerance will not be explored further. Same with diabetes mellitus, the severity of diabetes mellitus can be mild, moderate, or severe based on random blood glucose readings or HBA1c. For the purposes of IV Methylprednisolone we define this as the depth of resolution of our fault tree.

The corresponding fault tree is shown in Fig. 2.7.

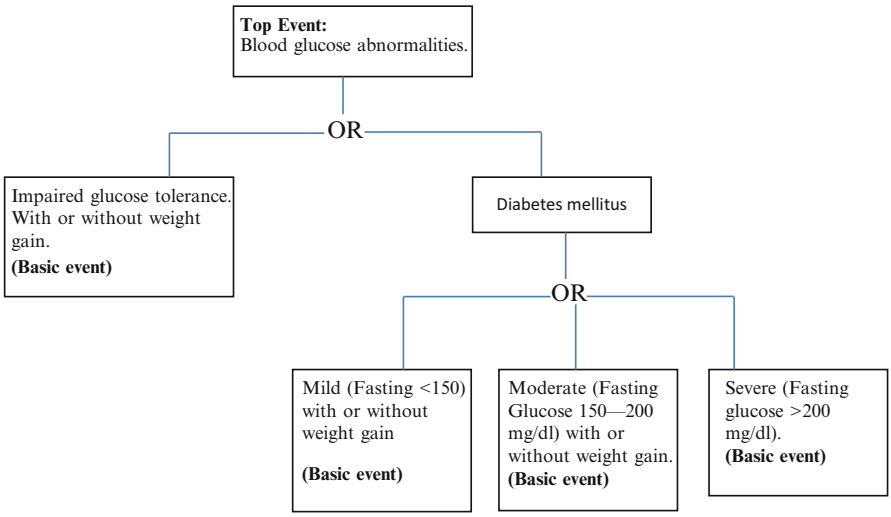

Fig. 2.7 FTA for the top event of blood glucose abnormalities with IV Methylprednisolone therapy for planned treatment of CIDP

3.5. FMEA for adverse side effects of IV Methylprednisolone therapy

Following the methods introduced in Section "FMEA for Lack of Therapeutic Efficiency", FMEA can be performed as follows.

(a) **Introductory statement** containing a statement about the purpose and objective of the FMEA: The objective of this FMEA is to describe the cardiovascular and endocrine adverse side effects, failure severity, exacerbating conditions, and mitigation strategies associated with adverse side effects of IV Methylprednisolone therapy.

(b) **Description of how the analysis was performed**: This analysis was performed based on a review of the literature detailing the experience of other investigators with the use of IV Methylprednisolone [8, 9] for CIDP and other autoimmune diseases. Failure modes from prior experience with steroid use in conditions such as myasthenia gravis, rheumatoid arthritis, systemic lupus erythematosis (SLE) were also incorporated into the analysis based on assumed similarities.

Assumptions: (1) The treatment trial will be limited, therefore only clinical concerns relevant to a time frame of 8–12 weeks of treatment are being considered.

Limitations of the FMEA include lack of rigorous quantitative data; limiting analysis to more immediate and frequently encountered failure modes, and not incorporating long-term consequences of immunosuppression such as malignancy, osteoporosis, aseptic necrosis of the hip, etc.

Table 2.4 FMEA report for cardiovascular and abnormal blood glucose adverse side effects of IV Methylprednisolone therapy for CIDP

Function name	Failure mode	Failure environment (obesity, prior diabetes, hypertension, CHF)	Failure severity	Mitigation strategies	Comments
Cardiovascular	Tachycardia	All populations	Minor	Monitor pulse rate	Patient education for mitigating anxiety
Cardiovascular	Electrolyte abnormalities/ hypokalemia	All populations	Minor (generally)	Monitor electrolytes, especially in combination with diuretics	Monitor closely
			Major in prior CHF		
Cardiovascular	Decompensated CHF	CHF patients	*Major*	Monitor cardiac status, weight gain, edema, dyspnea, orthopnea	Avoid therapy in high-risk populations
			Catastrophic		
Cardiovascular	Edema	CHF patients, prior edema	*Major*	Restrict salt, monitor weight daily	None
Cardiovascular	Hypertension	All populations	Minor (generally)	Restrict salt. Check blood pressure daily. Provide prescriptions for anti-hypertensives. See Chap. 9 for defense in depth	*If experiencing symptoms such as headache, shortness of breath, chest pains go to ER*
			Major in crisis		
Endocrine	Impaired glucose tolerance	Obese patients, prior borderline diabetes cases	Minor	Monitor glucose. Reduce added sugar and calories. Monitor weight	Rarely needs addition of Metformin
Endocrine	Mild diabetes mellitus	Obese patients, prior borderline patients	Minor	Monitor glucose. Reduce added sugar and calories. Monitor weight	Add metformin
Endocrine	Moderate diabetes mellitus	Obese patients, prior mild diabetes	Minor	As above, add Glipizide or sliding scale insulin	Request primary care assistance
Endocrine	Severe diabetes mellitus	Obese patients, prior poorly controlled diabetics	*Major*	As above	Request endocrine consult and partnership

As seen in column 4, the PSSA process shows one failure mode with potentially catastrophic consequence, three failure modes with major consequence in special populations with the rest of the failure modes being minor

(c) **A complete listing of results of the FMEA**: This is shown in Table. 2.4.
(d) **Appendices**: *Expanded list of side effects, including those not analyzed in this FMEA associated with pulse methylprednisolone therapy are listed in the prednisone FMEA in Chap. 4* [8, 9].

FMEA header information: see 3.5a, 3.5b, 3.5c, and 3.5d.

The advantage of performing an FMEA is it provides us the ability to identify potentially high-risk situations with major failure consequences, direct prevention and mitigation strategies appropriately. This approach was adopted in the use of pulse methylprednisolone for treatment of CIDP patients discussed in Chap. 9.

Regulatory Perspective

The above sections described the SSA process. These methods are adopted by companies in product development. They are also used heavily in demonstrating compliance with safety in regulatory filings with agencies such as the United States Federal Aviation Authority (FAA). Table 2.5 demonstrates the failure conditions and corresponding regulatory requirements required by the US FAA. Consider columns 2 and 5 from the table. Column 2 describes a system whose failure has no safety consequences. Examples include malfunction of the in-flight entertainment system. Such an event has no restriction on how frequently it can occur, systems concerned with it may be built to the lowest DAL (Level E). Regulatory compliance can be demonstrated by performing a FHA and design review. Column 5 deals with a system with severe safety consequences which can result in hull loss and multiple fatalities. Examples include Primary Flight Computers (PFC). Consequently, regulatory filings mandate demonstrating that the average probability of failure per flight hour of such a system be less than one in ten billion with FHA, FMEA data used in a detailed FTA to show that the event is extremely remote. The corresponding system also has the highest DAL—Level A.

Appendices

To make this introduction of FTA self-contained, the following sections look at further theoretical aspects of fault trees. These are useful to understand the principles behind software and computer-based FTA packages.

Table 2.5 United States Federal Aviation Administration: AC 25.1309 regulatory requirements for demonstrating safety of airplane systems

Harmonized 25.1309 Requirements and Compliance Summary					
Effect on airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on occupants excluding flight crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on flight crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Classification of failure conditions	No safety effect	Minor	Major	Hazardous	Catastrophic
DO-178B S/W and DO-254 H/W Levels	Level E	Level D	Level C	Level B	Level A
Allowable qualitative probability	No probability requirement	Probable	Remote	Extremely remote	Extremely Improbable
Allowable quantitative probability	10^{-3}	10^{-5}	10^{-7}	10^{-9}	
	Average probability per flight hour (or per flight if less than 1 h) on the order of:				
System Compliance Method: (common cause hazards not conductive to numerical analysis, such as foreign object collision, human error, etc. may be analyzed primarily by design review)	*FHA & Design Review*: Design, functional separation, and implementation reviewed to ensure failures will only produce no safety effect	*FHA & Design Review*: Design, functional separation, and implementation reviewed to ensure failures will only produce minor effect	*FHA, Design Review & FMEA Review*: Failure modes and effects analysis reviewed to ensure that failure effects of components involved in the function and failure rates are appropriate for major category	*FHA, Design Review and Fault Tree Analysis (FTA)*: FMEA & FHA data combined in detailed FTA to validate that the system probability of hazard is extremely remote	*FHA, Design Review, and FTA*: FMEA and FHA data combined in detailed FTA to validate that the system probability of hazard is extremely Improbable

(continued)

Table 2.5 (continued)

Harmonized 25.1309 Requirements and Compliance Summary		
Effect category validation	All functional hazards should have a multidisciplinary review by experts representing the engineering and operational areas. Where functions are the same as previous airplanes, past experience should be reviewed. Other conditions should be evaluated in lab and simulation tests. Failures affecting handling qualities will be evaluated in piloted simulation and/or flight test	Specific failures may be evaluated by piloted simulation as necessary

Conditions with increasing impact on safety are listed from left to right. The corresponding allowable probability of failure, DAL, compliance methods for demonstrating safety are described in the rows at the bottom of the table. Courtesy: Dr. Ying C Yeh, unpublished work, Boeing Company

Appendix 1: Evaluating Fault Trees—Failure Sequences, Probability Basics, and Boolean Algebra

Sometimes, system failures must occur in a specific sequence for the top event to happen. As a medical example consider the clinical situation of fracture of the femur (Failure A) which leads to nerve damage (Failure B) followed by damage to the blood vessels from bone fragments (Failure C) followed by blood loss (Failure D) followed by shock (Failure E) followed by fat embolism syndrome (Failure F) followed by altered mental status (Failure G) and then death (top event). The top event of death in this medical example happened because of events happening in that sequence. This is shown in Fig. 2.8.

The following sections explore probabilistic analysis and simplification of fault trees. Fault trees are analyzed using Boolean algebra and probability theory. A few basic concepts applicable to fault trees are presented here. Important rules of Boolean algebra and important probability theory basics applicable to fault trees and mathematical understanding of reliability are discussed in the next two sections.

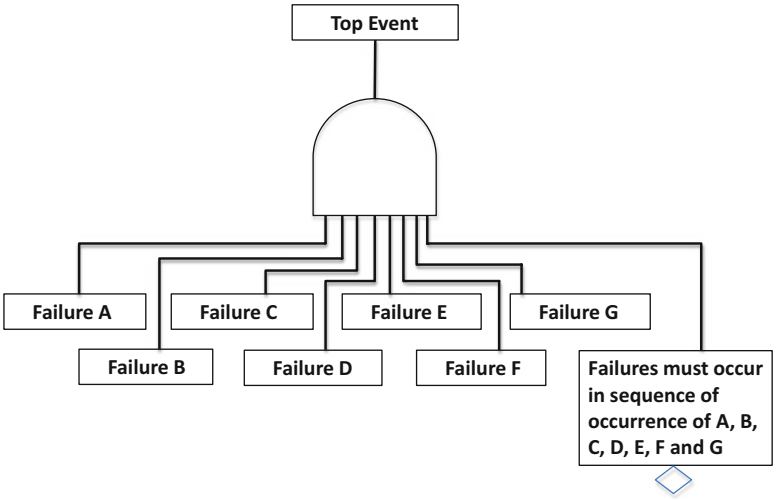

Fig. 2.8 Example of a specific sequence of failures causing the top event. The failures must occur in sequence and they are represented as inputs to an AND gate from left to right with the failure sequence condition represented on the far right as an undeveloped event (with a *diamond* symbol). In general there are $n!$ sequences (n factorial, represented by the symbol! refers to $n \cdot (n-1) \cdot (n-2) \ldots 1$, for example $3! = 3 \cdot 2 \cdot 1 = 6$) in which n systems can fail, therefore a restriction to k possible failure sequences reduces the probabilities by $k/n!$

Important Probability Distributions Used in Fault Trees

For FTA and in reliability theory, a few probability distributions are of great importance. These include the binomial and a special case of the binomial—Poisson. This leads to the exponential distribution which is frequently used to model failure. Some important aspects are presented here, a full discussion of the mathematical concepts is presented in [4].

Consider the example of an experiment which involves tossing a coin "three" times. Let the probability of getting a heads on any one trial be p. Therefore the probability of getting tails is $(1-p)$. The following outcomes are possible (H denotes Heads, T denotes Tails): HHH, HHT, HTH, HTT, THH, THT, TTH, and TTT (eight possible outcomes). HHT, HTH, THH are unique sequences where two heads occur in three trials. Similarly TTH, THT, and HTT are unique sequences where one heads and two tails occur in three trials. 3 heads or 0 heads occur in 1 out of 8 ways each. If we are interested in the case of getting two heads in three trials, the probability of getting two heads is p^2 and one tails is $(1-p)$ for one such sequence. This can be expressed as $p^2(1-p)$ However, there are three such sequences. Therefore the total probability is $3(p^2(1-p)))$. For the general case of n trials for a random variable x, with probability of success p in one trial, the probability of k successes is given by the *Binomial distribution*. This is given by the formula expressed as [6]:

$$b(k;n,p) = \binom{n}{k} p^k (1-p)^{n-k} \tag{2.4}$$

where $\binom{n}{k}$ denotes the number of ways of choosing k out of n items and is given by$\frac{n!}{(n-k)!\,k!}$ [6]. The average number of successes, expressed as λ, is n multiplied by p or np. If the individual probability of success is very low, the number of trials n is very large, the binomial can be approximated by the Poisson distribution which is given by:

$$p(x;\lambda) = \frac{\lambda^x \mathrm{e}^{-\lambda}}{x!} \quad \text{for} \quad x = 0, 1, 2, \ldots \tag{2.5}$$

In Eq. (2.5), e is the natural logarithm with an approximate value of 2.71828 to the first five places of decimal. The Poisson distribution lends itself well to modeling problems in reliability and component failures. If we have a "failure rate" or an "occurrence rate" where α failures occur per unit of time θ, we can determine probabilities of x failures in time t. The new average number of failures λ is given by $\alpha t/\theta$. For example, a light bulb manufacturer reports four light bulbs in a lot will fail every 100 h. If we are interested in determining what is the probability of six failures in 400 h of operation, we calculate λ as $\frac{4\times 400}{100} = 16$. Substituting this value into Eq. (2.5)

$$p(6;16) = \frac{16^6 e^{-16}}{6!} = 0.0026 \tag{2.6}$$

The special case of 0 failures is reliability. The *reliability* of a system $R(t)$ is defined as the probability of continuous successful operation for a time t. Therefore:

$$R(t) = P(0 \text{ failures in time } t).$$

Expressing λ by $\alpha t/\theta$, $x = 0$ in Eq. (2.5), we get:

$$p(x;\lambda) = \frac{\frac{\alpha t^0}{\theta} e^{-\frac{\alpha t}{\theta}}}{0!} \tag{2.7}$$

The first term $\alpha t^0/\theta$ is 1 since it is raised to the power of 0. The denominator 0! is 1. Therefore the above expression for reliability simplifies to:

$$R(t) = e^{-\frac{\alpha t}{\theta}} \tag{2.8}$$

If we use the symbol μ to represent $\frac{\alpha}{\theta}$, Eq. (2.5) is expressed as:

$$R(t) = e^{-\mu t} \tag{2.9}$$

If $R(t)$ is the probability of failure-free operation to time t, then $1 - R(t)$ is the probability of *at least* one failure in time t. In other words, reliability is the probability that the system will perform its specified functions for the specified time t. $F(t)$ represents the cumulative probability of failure in time t. From Eq. (2.9), this can be expressed as [4]:

$$F(t) = 1 - e^{-\mu t} \tag{2.10}$$

It is a measure of unreliability. Mathematical differentiation of this entity yields the corresponding probability density function (pdf) $f(t)$. This is the probability of failure between time t and $t + \Delta t$ [4].

$$f(t) = \frac{dF(t)}{d(t)} = \mu e^{-\mu t} \tag{2.11}$$

The expression for reliability $R(t)$, cumulative distribution $F(t)$, and pdf $f(t)$ are widely used in system analysis and reliability [4, 6]. These functions are closely interrelated. The reliability function is an exponential function which is a simple, easy-to-use distribution. Only one parameter—the failure rate $\mu\left(\frac{\alpha}{\theta}\right)$ specifies the distribution. Θ denotes the mean time to failure in this function. It is extremely important to note the assumptions, under which such a function was derived, the assumption of mutually independent trials and Poisson approximation to the binomial.

The failure rate function, also called hazard function, is a conditional probability distribution $\lambda(t)$ which provides information how a system is aging [4]. It indicates the changing failure rate with aging, for example, a new light bulb may have a 2 % chance of failing in the first 100 h. After this time, the failure rate may increase to 5 % between 100 and 200 h and to 10 % between 300 and 400 h. For a general distribution, the failure rate function is defined as:

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{2.12}$$

For the special case of the exponential distribution, substituting $f(t) = \lambda e^{-\lambda t}$ and $R(t) = e^{-\lambda t}$ in Eq. (2.12), we get

$$\lambda(t) = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$$

In other words, for the exponential, the failure rate function does not change with time. The components have a constant failure rate or in other words the probability of future failure is independent of the past operating time [4].

Boolean Algebra

Since fault trees are composed of events which either occur or do not occur (a component either fails or is functioning) connected by logical operators (especially OR and AND) they lend themselves to analysis using Boolean algebra. A fault tree can be viewed as a pictorial representation of the Boolean relationship between different variables. We review some of the basic relationships in Boolean algebra which are essential in the simplification of fault trees. More comprehensive rules of Boolean algebra are available in [4] or any of the many textbooks on the subject. Let us consider a pair of variables X and Y and explore the rules of Boolean algebra and their equivalent engineering symbolism. Let X be the set {2, 4, 6, 8} and Y be the set {1, 3, 6, 8, 9, 10}

1. $X \cap Y$: The set of elements which belong to X AND Y. This is also expressed as $X.Y$ (multiplication). For the example above $X \cap Y$ is the set {6, 8} which belongs to both X and Y. It follows that $X \cap X$ and $X \cup X = X$.
2. $X \cup Y$: The set of elements which belong either to the set X or to Y. For the example above, $X \cup Y$ is the set {1, 2, 3, 4, 6, 8, 9, and 10}. In engineering symbolism, this is represented at $X + Y$.

3a. $X \cap (X \cup Y) = X.\ (X + Y) = X$.

3b. $X \cup (X \cap Y) = X + X.Y = X$. Rules 3a and 3b are called the Law of Absorption.

4. It also follows that $X \cdot X$ and $X + X = X$.

5. $X \cap (Y \cap Z) = (X \cap Y) \cap Z$; in engineering symbolism $X.Y.Z.$ or $(X.Y).Z$ or $(X.Y).Z.$ This is called Associative law where the order of operations for the AND operator does not matter.

6a. $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$; in engineering symbolism $X + Y.Z = (X + Y).(X + Z)$.

6b. $X \cap (Y \cup Z) = (X \cdot Y) + (X \cdot Z)$; 6a and 6b are called Distributive law.

7a. $(X \cap Y)' = X' \cup Y'$; in engineering parlance $X' + Y'$.

7b. $(X \cup Y)' = X' \cap Y'$; in engineering parlance $X'.Y'$ (7a and 7b are called De Morgan's laws.)

The symbol X' represents the elements not in X. For conditions such as X represents the event of a component failure, X' represents the logical opposite that it is functional. $X \cap X' =$ the null set since a set cannot have any elements which are in it and not in it at the same time. In safety parlance, a component cannot be failed and functioning at the same time. $X \cup X'$ is the universal set since it represents all possible outcomes. If X and Y represent individual component failures, $(X \cap Y)$ represents the situation when both X and Y have failed, then $(X \cap Y)'$ represents the situation where a combined failure has not occurred. De Morgan's laws state that the event $(X \cap Y)' = X' \cup Y'$ can occur if X does not occur (X') or Y does not occur (Y') i.e., one or the other of X and Y are still functioning [4].

Now that we have reviewed the important Boolean algebra and probability theory basics applicable to fault trees, we proceed towards the development and analysis of fault trees.

FTA Development, Simplification, Minimal Cut Set *Determination*

Once a fault tree is created, it is simplified using Boolean algebra to determine the fault tree's "minimal cut sets." A "minimal cut set is the smallest combination of component failures which if they occur will cause the top event to happen." Simplification of fault trees using Boolean algebra helps avoid redundancies in their estimation. The combination of failures is the smallest necessary set of events needed for the top event to occur. All the failures in the minimal cut set are needed for the top event to occur. Consider the following fault tree example from Fig. 2.9 [4].

The tree can be described as a Top event called T. T happens if events E1 AND E2 happen. The tree is extended to the next level. E1 happens if event A OR event E3 happen. E2 happens if C OR E4 happen. The tree is then extended further to the next level. E3 happens if events B OR C happen. E4 happens if events A AND B happen. At this point, the limit of resolution of the tree is reached and it is not developed further. However, this tree can be simplified using the rules of Boolean algebra developed in the earlier section. Expressing events using the equivalent

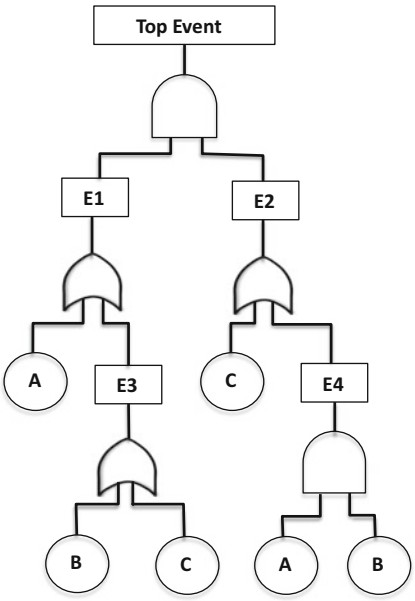

Fig. 2.9 Fault tree example from [4]. See description of events and logical operators above

logical AND (·), OR (+) operators, we can express the tree in the following Boolean algebra form:

$$T = E1 \,.\, E2 \tag{2.13a}$$
$$E1 = A + E3 \tag{2.13b}$$
$$E3 = B + C \tag{2.13c}$$
$$E2 = C + E4 \tag{2.13d}$$
$$E4 = A \,.\, B \tag{2.13e}$$

Substituting for E1 and E2 in the expression for T, we get

$T = (A + E3) \,.\, (C + E4)$ Multiplying and expanding the terms we get :
$T = A \,.\, C + C \,.\, E3 + A \,.\, E4 + E3 \,.\, E4$ Substituting for E3 (Eq. (2.13c)) we get :
$T = A \,.\, C + C \,.\, (B + C) + A \,.\, E4 + (B + C) \,.\, E4$ which simplifies to :
$T = A \,.\, C + B \,.\, C + C \,.\, C + A \,.\, E4 + E4 \,.\, B + E4 \,.\, C$

Now $C \cdot C = C$ and by the law of absorption (all the elements in a set are in common with itself), $A \,.\, C + B \,.\, C + C + E4 \,.\, C = C$. This can be understood somewhat intuitively. A . C, B . C, E4 . C are the elements which are common to A and C, B and C, and E4 and C respectively. These are therefore different subsets of C and when these are combined with the original set, we get the full set of elements in C.

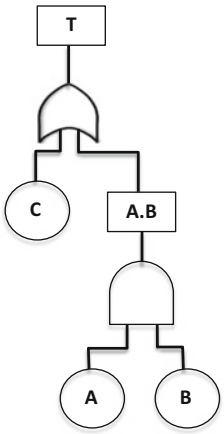

Fig. 2.10 Boolean algebra simplification of the fault tree in Fig. 2.9. T represents the top event

Using this simplification, we get:

$$T = C + A \,.\, E4 + B \,.\, E4 \quad \text{Now substituting for event E4 (Eq. (2.13e)), we get :}$$
$$T = C + A \,.\, (A \,.\, B) + B \,.\, (A \,.\, B) \quad \text{Again, applying the law of absorption we get}$$
$$A \,.\, A \,.\, B + B \,.\, A \,.\, B = A \,.\, B$$
$$T = C + A \,.\, B$$

This expression is considerably simpler than the original expression. This states that the top event T occurs if C happens alone OR A AND B happen together. Therefore the minimal cut sets of the top event are C and $A \cdot B$. The equivalent fault tree is shown in Fig. 2.10. The logical opposite or complement of the fault tree is the success tree. The minimal path set is the smallest combination of primary events whose nonoccurrence prevents the top event from happening. For the example above, the minimal path set can be derived by evaluating the logical opposite or complement of T. Let us denote this using the symbol T′.

$$T' = (C + A \,.\, B)' \quad \text{Using De-Morgan's theorem } (A \cup B)' = A' \cap B'$$
$$T' = C' \cap (A \,.\, B)'$$

Expanding the second term using De Morgan's laws $(A \cap B)' = A' \cup B'$ we get.

$$T' = C' \cap \left(A' \cup B'\right) \quad \text{Using } + \text{ for } \cup \text{ and } (\cdot) \text{ for } \cap, \text{ we get :}$$
$$T' = C'A' + C'B'$$

In other words, the top event T will not happen if C does not happen AND A does not happen or C does not happen AND B does not happen.

A simple illustrative example which has the characteristics of the fault tree in Fig. 2.10 is the electrical circuit in Fig. 2.11.

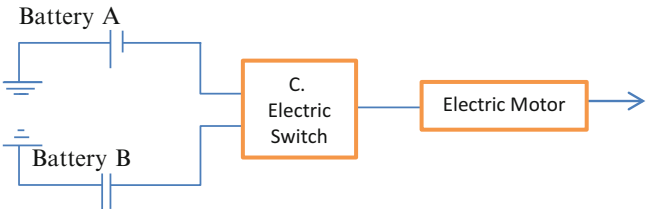

Fig. 2.11 Physical example of fault tree in Fig. 2.10. Battery A or B provides energy to run an electric motor. An electrical switching mechanism selects one of the energy sources to run the motor at any given time. Let T denote top event "No electricity to electric motor." The event A: Battery A fails, B: Battery B fails, C: Electric switch fails. The minimal cut set T happens if either the switching mechanism fails or both batteries fail $(A \cdot B)$ as shown in Fig. 2.10. The corresponding success tree, or "there is electricity to the motor" happens if the switch is functional C' AND Battery A is working $(A' \cdot C')$ OR Electric switch is working C' AND Battery B is working $(B'C')$. Adapted from [4]

Qualitative and Quantitative Evaluation of Fault Trees

Two broad types of results are obtained from fault tree evaluation: qualitative results and quantitative results [1, 4].

Qualitative Results

1. Minimal cut sets: Determine the smallest combination of component failures which can cause system failure. This forms the starting point for quantitative evaluations as well.
2. Qualitative importance: Qualitative ranking of contributions to system failure.
3. Common cause failure: Determine minimal cut sets which are susceptible to a single-component failure.

Quantitative Results

1. Numerical probabilities: Determine the failure probabilities of individual cut sets and calculate probability of system failure.
2. Quantitative importance: Quantitative ranking of contributions to system failure.
3. Sensitivity evaluations: Effects of changes in models and data, error determinations.

Qualitative Results

Minimal Cut Sets

As discussed earlier, in minimal cut set determination, the top event T is represented by an equation of the form:

$$T = F1 + F2 + F3 + F4 + \cdots$$

Assume F1 represents primary event A, F2 event B, F3 event C, F4 event (D·E), F5 event (F·G), F6 (H·I·J), F7 event (I·J·K·L), etc. Therefore:

$$T = A + B + C + (D \cdot E) + (F \,.\, G) + (H \,.\, I \,.\, J) + (K \,.\, L \,.\, M \,.\, N)$$

The top event T thus contains three single component system failures, F1(A), F2 (B) and F3(C); F4(D·E), and F5(F·G) constitute double event failures; F6 triple event and F7 quadruple event failures. The top event therefore has [4]:

three single component minimum cut sets
two double component minimum cut sets
one triple component minimum cut set and one quadruple component minimum cut set

Qualitative Importance

Ranking the minimal cut sets in order of their component size helps with understanding the importance of failures. Single cut sets are listed first, followed by double, then triple, etc. Most computer analysis of fault trees list failures in this order. Since computer complexity increases with size of the cut set, most failures list one, two, and three component minimal cut sets. Higher-order cut sets become important if they show susceptibility to common cause failures (this will be explored further).

Ranking cut sets by size is useful since failure probabilities associated with them decrease by several orders of magnitude as the size of the cut set increases. Let us assume any single component has a 1 in 1,000 chance of failing. Or in other words P (failure of a single component) $= 10^{-3}$. Therefore, a double cut set, which is the probability of two components failing is $10^{-3} \times 10^{-3}$ or 1 in one million. Extending this calculation to three element failures, we get $10^{-3} \times 10^{-3} \times 10^{-3}$ or 1 in one billion for three element minimal cut sets. Therefore, ranking minimal cut sets in terms of size provides a general idea of importance [1, 4].

In the design of fault tolerant systems, in many instances a required criterion for acceptable design or certification is *no single component failure can cause system failure*. The equivalent statement in fault tree terminology is that there are no single component minimal cut sets. The minimal cut sets can be checked to see if this is satisfied [1, 4].

Common Cause Susceptibilities

Common cause susceptibility looks at single failures which cause more than one primary event in the minimal cut sets to occur which can fail the system. A single basic cause may cause multiple failures which can fail the system. In evaluating common cause susceptibility, we are interested in common causes which can trigger all the primary failures in a minimal cut set. This can be performed by identifying common cause categories which can cause component dependence [4]. Common categories of common cause susceptibilities include environment (temperature, humidity, dust, contamination, etc.), manufacturer and operator among others. For example, water main burst causing flooding can cause failure of multiple electrical systems causing all the primary events in a minimal cut set to occur. Another example involves multiple similar components manufactured by the same manufacturer which may fail due to similar manufacturing defects. Software is another potential vulnerability. Once such common cause susceptibilities within categories are identified, the next step is to identify the minimal cut sets whose primary failures are all vulnerable to common cause failure. The minimal cut sets determined to be susceptible to common cause vulnerability are then screened for further action [1, 4].

Quantitative Evaluation of Fault Trees

Following the identification of minimal cut sets, probability evaluations can be performed to provide numerical estimates of probability of system failure. This is performed in a hierarchical fashion, component failure probabilities are first calculated, followed by minimal cut set probabilities followed by the top event or system failure probability [4]. Probabilities are calculated across logical OR and AND gates using rules discussed earlier. This is of course a simplistic description; in actual practice this is substantially more complicated. Common probability models are constant failure rate/h (λ) models—region II of the reliability curve in Chap. 1. The higher failure rates seen during "burn in" and "wearing out" are ignored in this analysis. When time varying models to account for these or a greater precision is required, more sophisticated models such as Weibull and Gamma probability distribution are preferred [4]. The relevant concepts of reliability $R(t)$, cumulative failure probability $F(t)$, and probability density function $f(t)$ were discussed in earlier sections. For small values of λt, $F(t)$ can be approximated by expanding $e^{-\lambda t}$ by its Taylor's series expansion:

$$e^{-\lambda t} = 1 + \frac{-\lambda t}{1!} + \frac{(-\lambda t)^2}{2!} + \frac{(-\lambda t)^3}{3!} + \cdots, \quad -\infty < -\lambda t < \infty$$

Since $F(t) = 1 - e^{-\lambda t}$. For small $-\lambda t$, the higher-order terms can be ignored (since $(-\lambda t)^2$ is much smaller than $-\lambda t$ Therefore we get $F(t) = 1 - (1 - \lambda t)$. Or in other words, for small $-\lambda t$:

$$F(t) \cong \lambda t \quad \text{for small } \lambda \text{ (low failure rates) and } \lambda t \leq 0.1$$

The probability of a minimal cut set is the product of the individual basic event probabilities [1, 4, 5]. The probability of the top event is the sum of the products of the individual probabilities [5]. This is called the sum of products approximation [5]. This is expressed as follows [5]:

$$P(\text{top event}) = \sum P(\text{Minimal cut sets})$$
$$P(\text{Minimal cut set}) = \prod (\text{Basic events in that particular minimal cut set})$$

where $\prod$ denotes multiplication A toy example for an AND gate is given in Fig. 2.12.

For systems whose operating life involves stand-by and active modes, the failure rate is defined as [5]:

$$\lambda = \lambda_0 d + \lambda_N (1 - d)$$

where d is the fractional duty cycle or (total operating time/total mission time), λ_0 is the component failure rate in the operating state, λ_N is the contribution to component failure rate from nonoperating state [5]. Stand-by modes are important in the analysis of latent failures. Conceptually, if a service requires two systems A and B where A is in use most of the time and B is used only if A fails (therefore is a stand-by), a failure involving B would not be detected during the normal operation of A. Since this failure is hidden, it is termed latent failure. Although it does not reduce service delivery, it degrades the safety margin of the system. In general, latent failures can affect systems whose functions are not required during normal operation but provide fail-safe coverage or protection against abnormal operating conditions [1]. The interval between when such a backup system was last known to be operating normally and when it will operate normally again is called exposure time. Such systems require maintenance checks, self-check tests for early detection, and repair to reduce exposure times [1] (Fig. 2.12).

Sensitivity Evaluation

Fault trees can help an analyst estimate how sensitive a system is to particular primary events. Numerical estimation of fault trees using different component failure rates or different exposure times can help with determining if more expensive components can significantly reduce probability of system failure or determine the appropriate maintenance intervals. Quantitative importance for determining the

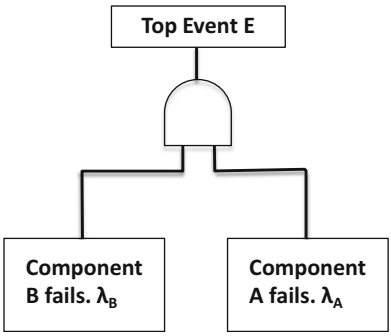

Fig. 2.12 Toy example of quantitative analysis of fault trees. The top event E happens if components A and B fail together. Assume exponential distribution with constant failure rate. For small λ_A and λ_B, $F(t)$ can be approximated by λt. Therefore $P(\text{Top Event E}) = P(\text{Failure of A and B})$ in a given time t is given by $P(\text{A})\,P(\text{B|A})$. If A and B are assumed to be independent, this becomes $\lambda_A \lambda_B t^2$

relative importance of a minimal cut set to top event probability can be performed to rank events in order of their importance. Some methods of doing this are:

(a) Ranking cut sets in descending order of probability.
(b) Calculating cut set importance: for a particular minimal cut set, this is calculated using the formula $= \frac{P(\text{minimal cut set})}{P(\text{top event})}$. This calculates what percentage of the total failure probability is contributed to by the cut set under evaluation.

Other methods include Fussell–Vesley (FV) importance and Birnbaum importance. The interested reader is referred to [1] for further information.

Finally the results of the FTA are presented as a summary. There are numerous methods of doing this [1]. This can take the form of a table where different top events, their respective probabilities, whether safety criteria specified in the PSSA are met, etc. are addressed. The process is iterative, deficiencies identified are addressed and FTA performed again to see if all safety objectives are achieved.

Appendix 2: Dependence Diagrams

DD are similar to fault trees; they represent an alternate method of representing data in a graphical analysis method similar to fault trees. The basic logic operations as in fault trees are OR and AND. However, instead of using logical operator symbols, an alternate method of using serial or parallel linkages between primary events is used. DD are analyzed in a manner qualitatively and quantitatively very similar to FTA [4]. DD are also called reliability block diagrams. The blocks themselves represent system components, the lines represent connections between them. Consider the following toy example in Fig. 2.13 (adapted from [1]).

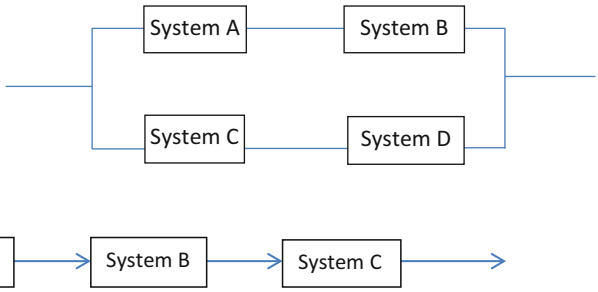

Fig. 2.13 Reliability block diagram

Fig. 2.14 Evaluating system reliability of a series connection of systems A, B, and C with individual reliabilities R_A, R_B, R_C. System reliability $= R_A R_B R_C$

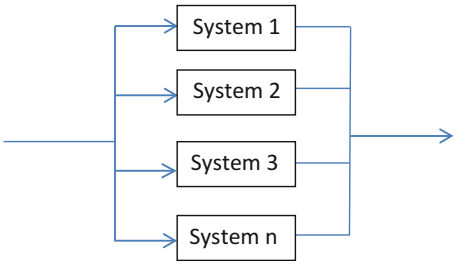

Fig. 2.15 Reliability of a parallel connection of component systems. If any of the systems is functioning, the output is delivered

Let $P(\text{A})$, $P(\text{B})$, $P(\text{C})$, and $P(\text{D})$ represent the respective failure probabilities of systems A, B, C, and D respectively. A series combination represents an OR gate and a parallel combination an AND gate. The top half of the figure shows a series combination of systems A and B. Therefore, a failure of either system A OR system B can cause failure of the top branch. Similarly, a failure of either system C OR D will cause failure of the bottom half. Both top AND bottom branches have to fail for overall system failure to happen. Represented mathematically:

$$\text{P(Failure)} = P(\text{A OR B failing}) \text{ AND } \text{P(C OR D failing)}$$

Applying the + operator for OR and $(\cdot)$ operator for AND we get:

$$P(\text{Failure}) = (P(\text{A}) + P(\text{B})) \cdot (P(\text{C}) + P(\text{D}))$$

The reliability of connected systems is assessed in a similar manner. For series connections (OR), the reliability of a combination is the product of individual reliabilities as shown in Fig. 2.14.

For parallel connections as shown in Fig. 2.15, the system reliability is evaluated differently. From the definition of reliability: Reliability $= 1 -$ System Failure [10].

For the entire system to fail, each of the individual systems has to fail. Let Ri) denote reliability of system i. For a particular system i, the failure probability is given by $1 -$ Reliability of System i $(R(i))$. Therefore, the probability of failure

of system 1 AND system 2 AND system 3. . .AND system N is given by the product of the individual failure probabilities [10].

$$\text{Probability of System Failure} = \prod_{i=1}^{n}(1 - R(i)) \text{ where}$$

$$\text{Reliability of the System, } R(i) = 1 - \text{Probability of System Failure}$$

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

Since the basic events are combined using logical OR and AND operators, DD lend themselves well to simplification using Boolean algebra [1] using the same rules as FTA. The analysis of DD involves Boolean algebra simplification to generate minimal cut sets and to perform qualitative and quantitative calculations on them.

Markov Analysis

MA is a method for analysis similar to FTA and DD. It is a powerful tool which can cover a wide range of system behaviors. A Markov chain represents various system states and transitions between them. The states themselves can be operational or nonoperational and the transition from one to the other is determined by the failure and repair rates. At any time, t the probability of being in a particular state can be calculated by solving a set of differential equations. The interested reader is referred to [1, 5] for further introduction to the topic.

References

1. ARP, SAE. 4761. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment 12; 1996.
2. Renaud S, Fuhr P, Gregor M, Schweikert K, Lorenz D, Daniels C, Deuschl G, Gratwohl A, Steck AJ. High-dose rituximab and anti-MAG-associated polyneuropathy. Neurology. 2006;66(5):742–4.
3. ARP, SAE. 4754. Certification considerations for highly-integrated or complex aircraft systems; 1996.
4. Roberts NH, Vesely WE, Haasl DF, Goldberg FF. Handbook, fault tree. NUREG-0492. US Nuclear Regulatory Commission; 1981.
5. Vesley W, Dugan J, Fragole J, Minarik II J, Railsback J. Fault tree handbook with aerospace applications. NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington DC; 2002.
6. Miller I, Marylees M, John E. Freund's mathematical statistics with applications. Pearson Prentice Hall: Upper Saddle River; 2004.
7. Traverse P. System safety in a few nutshells. ERTS Embedded Real Time Software 2008. Toulouse, France; 2008.

8. Lopate G, Pestronk A, Al-Lozi M. Treatment of chronic inflammatory demyelinating polyneuropathy with high-dose intermittent intravenous methylprednisolone. Arch Neurol. 2005;62(2):249–54.
9. Sinha A, Bagga A. Pulse steroid therapy. Indian J Pediatr. 2008;75(10):1057–66.
10. Reliability block diagram. http://www.win.tue.nl/~mchaudro/sa2007/Reliability%20Block%20Diagrams.pdf. M.R.V. Chaudron. Accessed 1 June 2013

http://www.springer.com/978-3-319-14967-7

Dependability in Medicine and Neurology
Using Engineering and Management Principles for
Better Patient Care
Balakrishnan, N.
2015, XV, 335 p. 76 illus., 45 illus. in color., Hardcover
ISBN: 978-3-319-14967-7