CHAPTER 36

SYSTEM SAFETY

36-1 INTRODUCTION

System safety is an approach to accident prevention that involves the detection of deficiencies in system components that have a potential for failure or an accident potential. System safety is the application of technical and managerial skills to the systematic, forward-looking identification, and control of hazards throughout the life cycle of a system, project, program, or activity. In this context, a system is an item of equipment or a process. Examples of complex systems are aircraft, weapons, production plants, vehicles, and buildings.

Chapter 3 discussed preventive strategies for accidents. A preventive strategy (Figure 3-4) does not allow accidents to happen before something is done about them, which is contrasted with a reactive strategy (Figure 3-3) that acts after accidents have occurred. The latter is costly and often ineffective, because an existing design and system limit what changes are easy to make. The farther in the development process that changes are made, the greater the costs (see Figure 36-1). Because of cost to change or a preexisting feature of a current system, the changes may not be as comprehensive or as integrally tied into a system as would be desired.

The key element in system safety is hazard analysis. The process identifies, anticipates, and controls hazards. The hazard analysis may consider the entire life cycle of a system. Many kinds of controls extend from the hazard analysis. They may be engineering controls that modify a system to eliminate or reduce the hazards to acceptable levels. Controls include management policy and procedures and identification and implementation of training for system operators, maintainers, and support staff. Controls may include operating procedures, emergency response, and other plans and application of many consensus standards and government standards and regulations for safety.

System safety is not just failure analysis. Hazard analysis may use failure analysis and other analyses to identify hazards, but system safety is a process for safety specialists to identify and deal with safety problems. System safety procedures often include risk assessment, which was discussed in Chapter 35.

The concepts for system safety evolved with aircraft and missile projects in the 1950s and 1960s. There were only a few models built during prototype phases, so design and testing could not afford very many failures or the program was ended. Even production models could not afford many failures, because the aircraft and missiles were very expensive and were a matter of much public attention. Therefore, hazards and failures had to be eliminated or reduced during the design and development phases.

Today, system safety concepts are incorporated in product design, building and facility design, accident prevention management, and other applications. Many system safety

Safety and Health for Engineers, Second Edition, by Roger L. Brauer

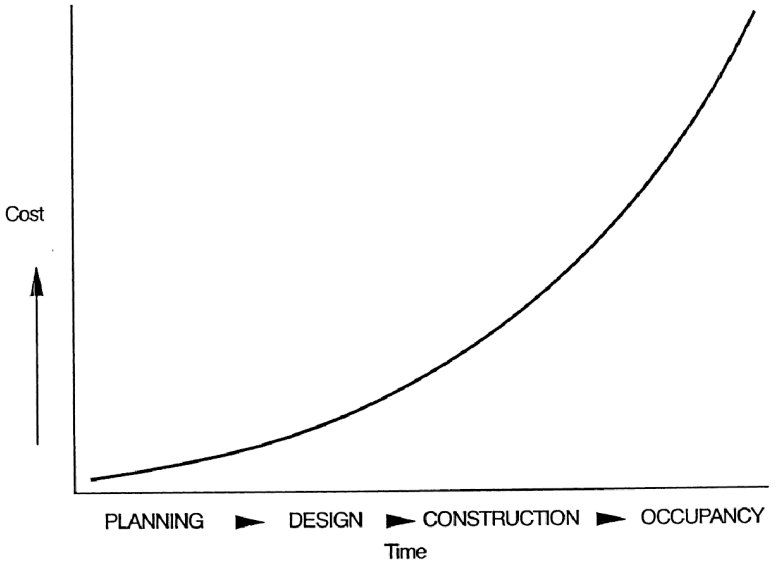

Figure 36-1. Cost for changes increase with stage of development.

techniques are integrated into process safety (see Chapter 30). Some of these applications are discussed further.

36-2 GENERAL PROCEDURES

Presented herein are examples of generally applied system safety procedures.

OSHA Process Safety Standard

The OSHA Process Safety Standard[1] incorporates many system safety concepts. For example, the standard calls for an experienced team to identify and analyze hazards (process hazard analysis, or PHA) using one or more of the following methods:

- What-If
- Checklist
- What-If/Checklist
- Hazard and Operability Study (HAZOP)
- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis
- An appropriate equivalent method

The analysis is then used to address

1. the hazards of the process
2. identification of previous incidents that had a potential for catastrophic consequences in the workplace
3. engineering and administrative controls

4. consequences of failure of engineering and administrative controls
5. facility siting
6. human factors
7. qualitative evaluation of possible safety and health effect of control failures

The final step is establishing a system to address the team's findings and recommendations in a timely manner through an action plan and schedule.

Military Standard 882

There are many variations in system safety procedures as they are applied by different organizations to a variety of systems. Military Standard 882 (MIL-STD 882) addresses an approach for management of environmental, safety, and health mishap risks encountered in the development, test, production, use, and disposal of systems, subsystems, equipment, and facilities. Those engaged in military acquisitions have used the procedures in MIL-STD 882 for a long time to identify, evaluate, and mitigate to an acceptable level mishap risks.

The standard defines a *mishap* as an unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. A *mishap risk* is the possibility and impact of a mishap expressed in terms of potential mishap severity and probability of occurrence. The standard defines *safety* as the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. It also defines a *system* as an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective. In addition, *system safety* is the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

The standard outlines requirements for the application of system safety to include:

- Documentation of the system safety approach, including
  - — Identification of processes used
  - — Integration of the approach into the overall program
  - — Defining how hazards and residual mishap risk are communicated to and accepted by authorities and are tracked
- Identification of hazards
- Assessment of mishap risk
- Identification of mishap risk mitigation measures, including (these are often referred to as "design order of preference"; see also Chapter 9)
  - — Elimination of hazards through design selection
  - — Incorporating safety devices
  - — Proving warning devices
  - — Developing procedures and training
- Reduction of mishap risk to an acceptable level
- Verification of mishap risk reduction
- Review of hazards and acceptance of residual mishap risk by authorities
- Tracking of hazards, their closures, and residual mishap risk

The standard outlines system safety management methods that may be required in procurements. It references the *System Safety Analysis Handbook*[2] as a publication covering system safety methods. The standard provides suggested classifications for mishap severity categories (see Table 36-1) and for mishap probability levels (see Table 36-2). Classifications from these tables then are used in combination to make decisions. One decision step is to establish mishap risk assessment values, which are used to rank different hazards in terms of mishap risk and to group hazards into mishap risk categories. A second step is to establish risk categories, which help to create specific actions for managing mishap risks. Table 36-3 is an example of a table of mishap risk assessment values, and Table 36-4 is an example of a table of mishap risk categories and mishap risk acceptance levels.

TABLE 36-1 Suggested Mishap Severity Categories

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1 million, or irreversible severe environmental damage that violates laws or regulations.
Critical	II	Could result in permanent partial disability, injuries, or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200,000 but less than $1 million, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $10,000 but less than $200,000, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2,000 but less than $10,000, or minimal environmental damage not violating law or regulation.

TABLE 36-2 Suggested Mishap Probability Levels[a]

Description[b]	Level	Specific Individual Item	Fleet or Inventory[c]
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but more than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible

[a] The probability that a mishap will occur during the planned life expectancy of a system, quantified in terms of potential occurrences per unit of time, events, population, items, or activity.
[b] Definitions of descriptive words may be modified based on quantity of items involves.
[c] The expected size of the fleet or inventory should be defined before accomplishing an assessment of the system.

TABLE 36-3 Example Mishap Risk Assessment Values

	Severity			
Probability	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

TABLE 36-4 Example Mishap Risk Category and Mishap Risk Acceptance Levels

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1–5	High	Component acquisition executive
6–9	Serious	Program executive officer
10–17	Medium	Program manager
18–20	Low	As directed

36-3 FAULT TREE ANALYSIS

Fault tree analysis is one system safety method often used for complex systems. Fault tree analysis, which was originated by H. A. Watson at Bell Telephone Laboratories in 1962,[3] is a boolean logic concept that evaluates *events*. The procedure relies on building a tree structure as shown in Figure 36-3. At the top is the principal or top undesired event, which is broken down into contributing factors that are further subdivided into event causes. Fault tree analysis is a deductive process that moves from the general to the specific. Combinations of events are considered in the causal chain. Interactions between events and elements of the system are a vital part of this method.

Fault tree analysis as applied to system safety relies on preliminary hazard analyses (PHA) or other analysis techniques to identify major undesirable events. The tree is developed further from PHA and other analyses. After the tree is constructed, qualitative or quantitative analysis is performed. To perform quantitative analysis, a probability must be assigned to each event cause. Today, computer systems make the procedures of constructing and analyzing fault trees quite easy. Qualitative analysis provides insights into fault paths and critical event causes.

Limitations of Fault Tree Analysis

Analysis of a fault tree can be no better than the events identified for it. A major limitation of fault tree analysis is failure to identify all the events that may lead to a top event. Failure to include an event may simply be oversight, but it may also be lack of experience and knowledge of the system and its behavior or potential behavior. When a system is being developed and analyzed for failures and undesired events, one may not have insight into the kinds of things that may lead to faults and failures in the future or may not be experienced with materials and components used and their potential failure modes.

Another significant difficulty is assigning valid probabilities to event causes. Although considerable data on equipment performance are available from reliability engi-

FREQUENCY OF OCCURANCE	HAZARD CATEGORIES			
	I CATASTROPHIC	II CRITICAL	III MARGINAL	IV NEGLIGIBLE
A FREQUENT	1A	2A	3A	4A
B PROBABLE	1B	2B	3B	4B
C OCCASIONAL	1C	2C	3C	4C
D REMOTE	1D	2D	3D	4D
E IMPROBABLE	1E	2E	3E	4E

Hazard Risk Index	Suggested Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 2D, 3B, 3C	Undesirable (Management Activity decision required)
1E, 2E, 3D, 3E, 4A, 4B	Acceptable with review by Management Activity
4C, 4D, 4E	Acceptable without review

Figure 36-2. Example hazard risk assessment matrix. (From MIL-STD-882B.)

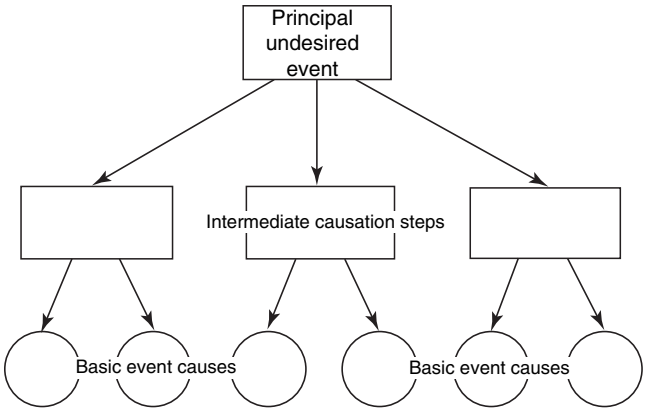

Figure 36-3. Fault tree concept. (Reprinted with permission from Roland, H. E., and Moriarty, B., *System Safety Engineering and Management*, John Wiley & Sons, New York, 1983.)

neering and other sources, placing probabilities on human activities with precision can be quite difficult. Humans may behave very differently under ideal conditions compared with stressful, boring, or distracting conditions. In addition, different people may act quite differently under the same conditions. Data banks on human errors provide reasonable information on simple human errors, but there is little information for estimating mistakes on higher-level tasks involving cognitive functions.

Another limitation on the use of fault tree analysis is cost. Compiling the knowledge for, constructing the fault tree, and assigning probabilities to tree elements can be laborious and costly.

Fault Tree Symbols

Fault tree analysis uses a particular set of symbols. Figure 36-4 illustrates commonly used symbols. There are some variations in symbology among practitioners.

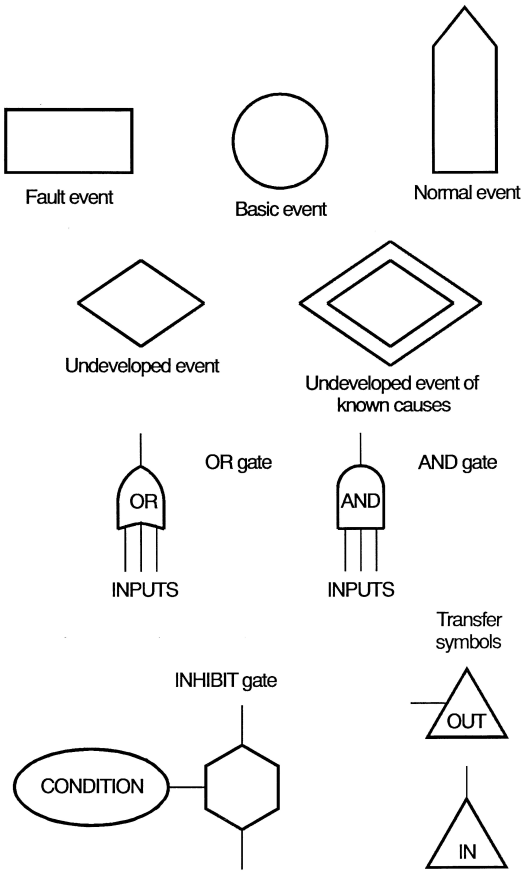

Figure 36-4. Symbols commonly used in fault tree analysis.

Events There are four kinds of events and symbols. A *fault event*, which is represented by a rectangle, is a top or intermediate event that must be described further in the tree. For quantitative analysis, a probability for a fault event is computed from elements below it in the tree.

A *basic event* is an event for which there will be no further analysis. It is represented by a circle and it is the terminus of a branch in the fault tree. Probabilities are assigned to basic events when quantitative analysis is performed.

An *undeveloped event* is represented by a diamond and is an event that an analyst chooses not to analyze. Although it may merit further analysis, an undeveloped event simply may be a curiosity or may not be critical to the problem at hand. Probabilities may be assigned to undeveloped events. Sometimes an undeveloped event of known cause is not developed further, but there is deeper knowledge about that branch of the tree. In diagraming such undeveloped events, some people use a double diamond.

A *normal event* is one that has two states: it occurs or does not occur. Normal events are represented by a house shape and are sometimes called *switch events*. In many cases, analysis of a tree should consider normal events in each of their two states. Frequently, normal events have probabilities of 1.0 or 0.0; sometimes other probabilities are assigned.

Logic Gates Because the elements in a fault tree are related by boolean algebra, symbols are used to depict the kind of relationship among elements. Basic logic relationships are

OR and AND, and are represented by gate symbols. Both AND and OR gate symbols have unique shapes.

An OR gate indicates that any one of the input events can cause an output event. When quantitative analysis is conducted, probabilities for input events attached to an OR gate are summed to compute the probability of the output event.

The other basic logic gate is an AND gate, which indicates that all of the input events must occur to cause the output event. In quantitative analysis, the probability of an output event is the product of all input events.

Special Notations There are other logical relationships that can occur in a fault tree. Various notations to AND and OR symbols indicate that special logical relationships or other symbols are used. For example, two input events for an OR gate may be mutually exclusive; that is, one excludes the other from occurring. An *exclusive* notation attached to the OR gate indicates this condition.

There may be a condition in which at least two of three input events are necessary for an output event to occur at an AND gate. A notation "$A_i \geq 2$" attached to the AND gate would note this special condition.

In another situation, one or more input events may have to occur before a third one has any consequence. This is called a priority modification. A notation "$C \rightarrow R_1, R_2$" would indicate that input event C is not significant unless input events R_1 and R_2 occur first.

Another variation, called a summation gate, is the possibility of having input events that must have certain levels before the output will occur. A summation gate may apply to either an OR or AND gate. A summation sign or note with the gate indicates this special condition.

Sometimes a complex array of conditions determines if an output event will occur at a gate. An "M" notation on a gate indicates that a complex matrix of conditions is processed by this gate.

For some events, certain conditions must be present for the input events to be included in the tree. The input events may inhibit or enable the output event. A hexagon symbol represents an inhibit gate.

When there is not enough space to complete a fault tree, it must be broken into parts. Discontinuities are represented by a transfer symbol that has the shape of a triangle. Identifying numbers or letters on both segments of a drawing indicate where they tie together functionally. A fault tree may have identical branches at more than one location. A transfer symbol reduces the need to completely represent the branches at each location in the tree.

Events

An event describes any element of a fault tree that represents an occurrence. Events may be normal events, failures or faults. Failures are attributes of components that interrupt the function of the component. For example, an electronic relay that sticks open is a failure event.

Fault events are events that contribute to component or system faults. A fault is a condition (not necessarily a failure) of a system, subsystem, or component that contributes to the possible occurrence of an undesired event. For example, failing to act in response to a fire alarm is a fault, but a deaf person not being able to hear an alarm is a failure.

There are four classes of causal events that appear in fault trees. Primary refers to internal attributes or conditions of components; secondary refers to something outside a component.

Primary Failures Primary failures are internal problems with components that make them inoperative. Repairing a primary failure returns a component to full operation. A primary failure also is defined as a failure of a component within the design envelope, such as an inherent characteristic of a component that causes the component to fail. The primary failure of one component cannot contribute to primary failure in another component.

Secondary Failures Secondary failures are external problems that make components inoperative. Repairing a secondary failure does not return a component to operation. A secondary failure is the failure of a component outside the design envelope, such as environmental conditions that affect a component. A primary or secondary failure of one component or a group of components can cause a secondary failure in another component.

Primary Faults Primary faults are events that are abnormal within an operation. They can lead to undesired conditions in a system.

Secondary Faults Secondary faults are event causations that are external causations. One form of secondary fault is a command fault: an inadvertent operation of a component resulting from failure of a control element. An example is accidentally bumping a control switch that energizes a circuit.

Constructing a Fault Tree

Development of a fault tree begins by selecting the top event. Usually, the top event is selected as the most important, most severe or most undesired event. The system to which the top event applies then is clearly defined and the state of the system must also be specified. Then one begins to construct the fault tree.

The first tier of events includes those that are necessary and sufficient causes for the top event. Other tiers are added, and then logical relationships among events are added. It is better to include generic causes at upper levels in a fault tree. This makes it easier to include detailed faults and failures in the tree structure.

Analyzing a Fault Tree

There are several approaches to analyzing a fault tree. Methods involve quantitative and qualitative analysis.

Qualitative Analysis of Fault Trees Creating a fault tree gives analysts insight into the causes of an undesired event and to system behavior. This alone may make the exercise worthwhile.

The elements of a fault tree can be evaluated to gain further insight into the causes of a top event. Causes within the tree can be evaluated and judgments can be made about the likelihood of faults or failures contributing to the top event. Each event sequence can be looked at, and those that are most likely can be considered first.

Another approach is to find the most likely sequences by analyzing the gates using products of input events for AND gates and sums of input events for OR gates. Products of values less than one are smaller than their sums. With this in mind, the most likely event sequence often can be identified quickly by tracing each branch of the tree from the top event to the bottom event. Branches linked by OR gates typically have high probabilities of occurrence, whereas branches linked by AND gates typically have low probabilities of occurrence.

Quantitative Analysis of Fault Trees Quantitative analysis begins at each bottom end of a branch. To perform quantitative analysis on fault trees, a probability must be assigned to each basic and normal event. Probabilities of occurrence may also be assigned to each undeveloped event.

Then boolean algebra is applied to each logic gate to determine the probability of each intermediate event. Ultimately, the analysis calculates the probability for the top event. Example 36-1 illustrates the fundamentals of this process for the fault tree shown in Figure 36-5.

Cut Sets Cut sets are any sequence of events (reading from the bottom of a branch to the top event) that leads to the occurrence of the top event. Each sequence that leads to the top event can be analyzed separately and then compared to the others. The comparison will help identify which sequence is most likely to cause the top event.

Example 36-1 For the fault tree in Figure 36-5, the probabilities for some of the events are as follows:

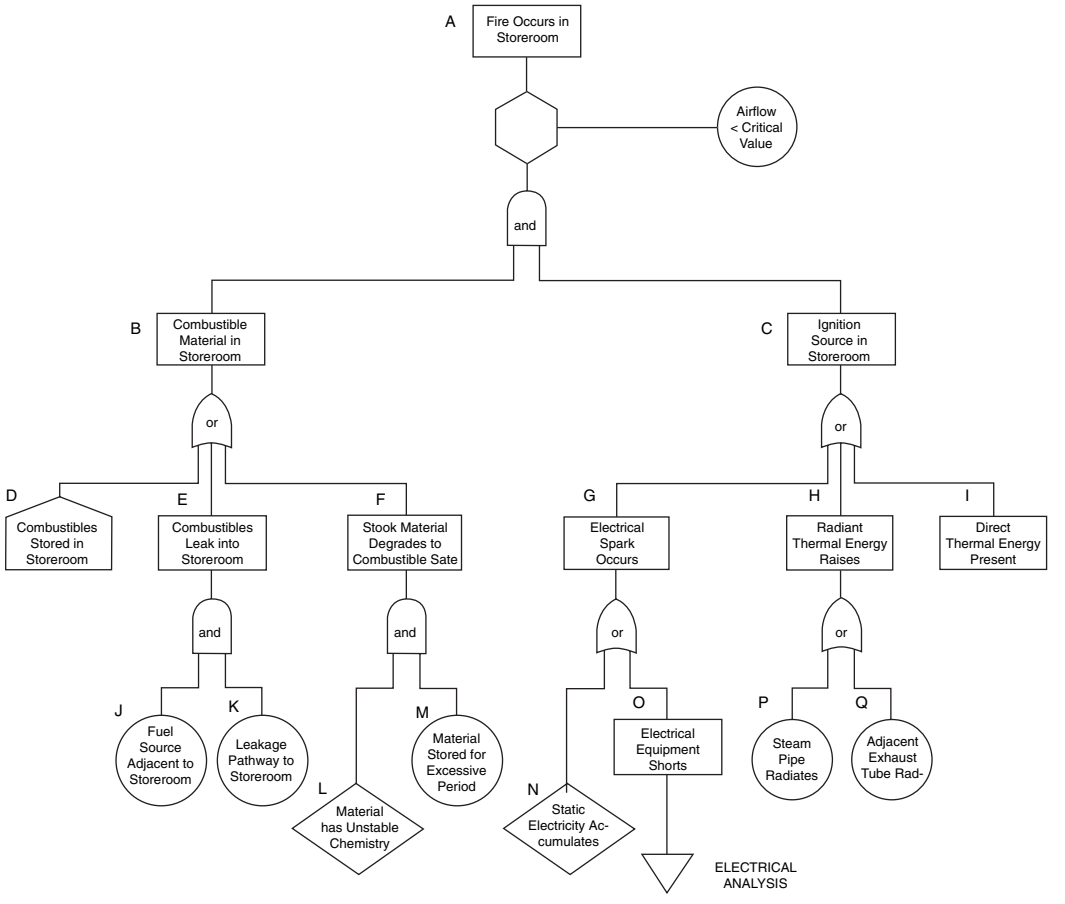

Figure 36-5. Example of a fault tree. (From *Facility System Safety Program Manual*, HNDP 385-3-1, U.S. Army Corps of Engineers, Huntsville Division, Huntsville, AL, October, 1985.)

Event	Probability for Events (Frequency in Days)
D	3.45×10^{-7}
J	6.89×10^{-4}
K	7.33×10^{-3}
L	6.05×10^{-3}
M	1.88×10^{-4}

What is the most likely cause for event B?

The probability for event D is given. The probability for event E is

$$P(J) \times P(K) = (6.89 \times 10^{-4})(7.33 \times 10^{-3})$$
$$= 5.05 \times 10^{-6}.$$

The probability for event F is

$$P(L) \times P(M) = (6.05 \times 10^{-3})(1.88 \times 10^{-4})$$
$$= 1.137 \times 10^{-6}.$$

Event E is the most likely cause. However, event F has a very similar probability and should be given careful consideration in selecting controls.

36-4 FAILURE MODE AND EFFECTS ANALYSIS

Failure mode and effects analysis (FMEA) is an inductive procedure that moves from the specific to the general. Examples of FMEA can be found in the form of diagnostic charts for automobile or appliance repair. The emphasis is not on events, but on conditions. FMEA analyzes *equipment* or *components*; it relates conditions of components to conditions of the system of which they are a part. Failures in components are traced to determine their effects on the system. Of greatest interest are effects that impact safety.

FMEA uses special tables and charts to log data during the analysis. One element of a typical worksheet is a *component description*. The worksheet identifies which individual or combinations of components are analyzed. The worksheet has a column for *failure mode*. Additional columns list *effects on other components* and *effects on the system*. The worksheet also contains a column to identify the hazard category (see Tables 35-2 and 35-3) or risk assessment code (see Figure 35-1). It may also estimate *failure frequency* and *effects probabilities*, which may be qualitative or quantitative. Finally, there is usually a column to identify *control method*, that is, to indicate how to prevent the failure or how to protect against its consequences.

In working across the data columns of a FMEA chart, it is important to recognize that there are many more relationships among data elements than one failure mode for each item, one cause for each failure, one effect for each cause, and so forth.

From a completed FMEA, a critical item list (CIL) can be developed. This list includes failures that exceed the acceptable levels of risk. The CIL may be used for more detailed safety analysis.

Figure 36-6 is an example of a FMEA worksheet.

36-5 SIMULTANEOUS TIMED EVENTS PLOTTING ANALYSIS

Another method for identifying hazards and relating them to systems is simultaneous timed events plotting analysis (STEP), which analyzes *events* from a time or sequence perspec-

FAILURE MODE AND EFFECTS ANALYSIS								
System		Subsystem		Date	Analyst		Page	
Component or Part Name/ Description	Failure Mode	Cause of Failure	Effect on...			Risk or Hazard Category	Probability of Effect	Comments
			Other Components	System	Personnel			

Figure 36-6. Example format for a Failure Mode and Effects Analysis (FEMA) worksheet.

tive. Sequences of events that occur quickly may require corrective actions different than those that occur more slowly. Event sequences that occur very slowly may be hard to recognize.

STEP procedures involve identifying people or things (called actors) and their actions. An actor plus an action is called an event. For example, "alarm sounds" and "occupant runs" are events. The events for each actor are plotted against a time line and relationships among different actors' events are identified by linking arrows. The resulting chart allows visualization of what events occur when there is a complicated sequence. Figure 36-7 illustrates a chart produced from a STEP analysis of a simple process.

36-6 HAZARD TOTEM POLE

Grose[4] applies system safety principles and techniques in preparing hazard control information for management decisions. His process begins by describing "scenarios" of things that go wrong for each organizational unit or functional element of an operation. The hazards in each scenario are identified and hazards are rated in each for (1) severity, (2) probability of occurrence, and (3) cost to correct. A table for each rating has four categories that are identified by letters instead of numbers. Hazard severity has categories A, B, C, and D, hazard probability has categories J, K, L, and M, and cost to correct has categories R, S, T, and U. Two of the tables have descriptions for categories very similar to those in Tables 35-2 and 35-3.

The combinations of categories from each of the three tables are organized into a decision chart called the hazard totem pole (see Figure 36-8). There are 64 levels in the totem pole (based on a $4 \times 4 \times 4$ matrix = 64 conditions). The totem pole is prepared separately from the evaluation of particular scenarios. At the top of the totem pole is the combination A, J, and R, which represents hazards that are very severe, have a high probability of occurrence, and are very inexpensive to correct. At the bottom of the totem pole is the D, M, and U combination, which represents hazards that are the least severe, are not very likely to occur, and are very expensive to correct. In between are the other combinations in an order acceptable to managers who make decisions about how much to spend on correcting hazards or an order based on risk and criticality, as depicted in Figure 35-1.

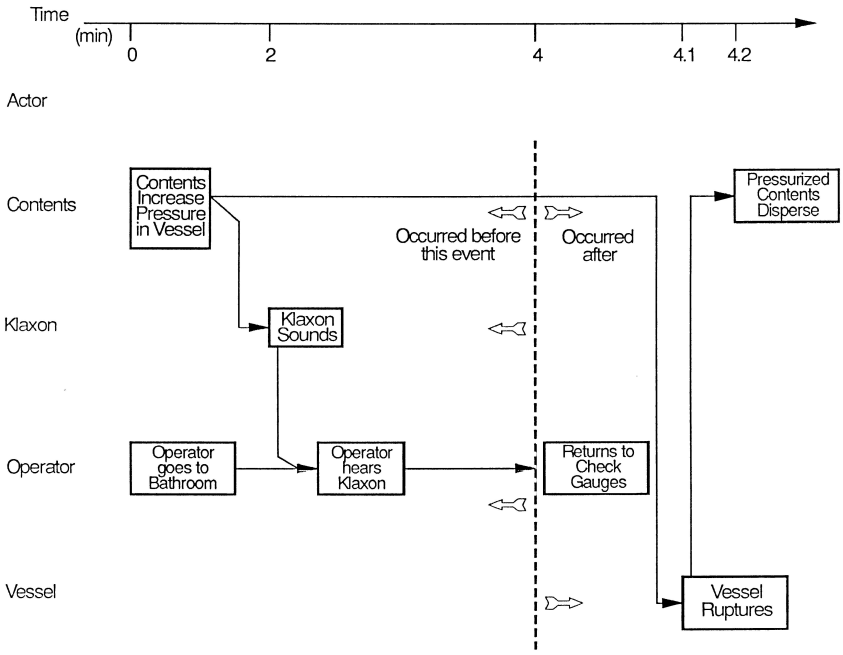

Figure 36-7. Example of a STEP analysis chart for a simple process. (From *Facility System Safety Program Manual*, HNDP 385-3-1, U.S. Army Corps of Engineers, Huntsville Division, Huntsville, AL, October, 1985.)

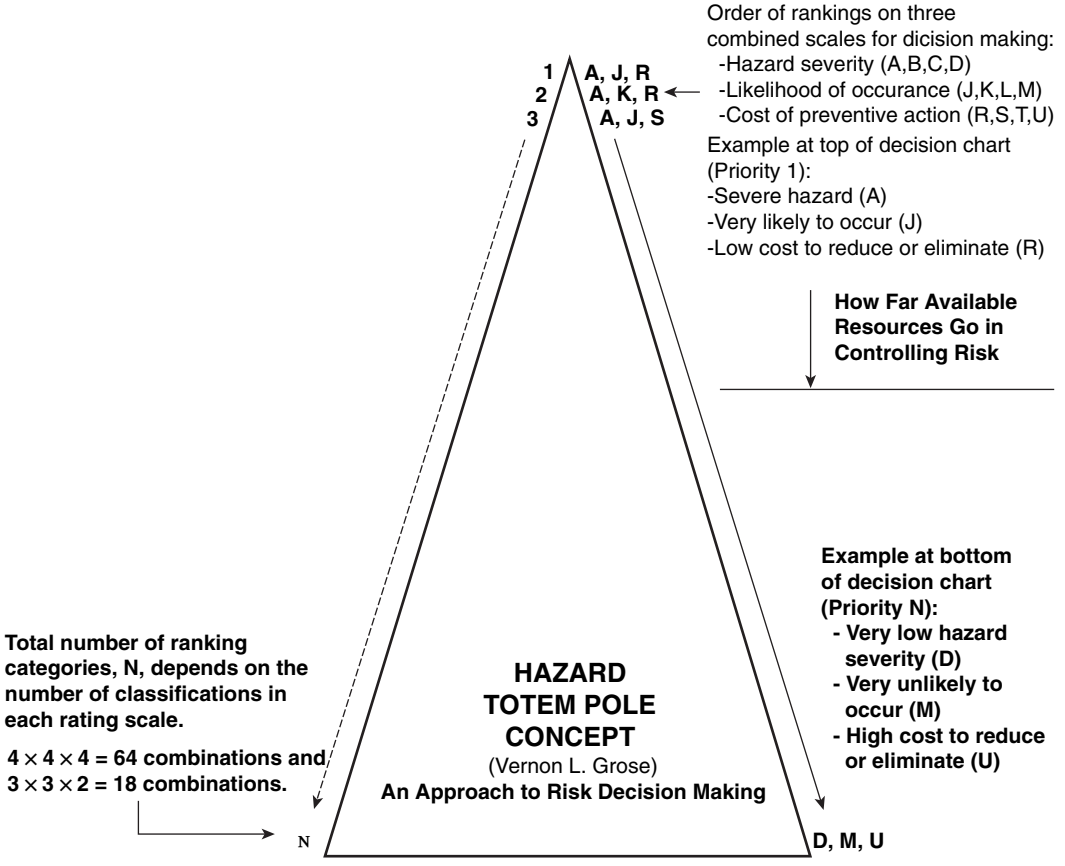

Figure 36-8. Hazard totem pole concept.

Hazards from the analysis of scenarios are organized in a list according to the combination of ratings established in the hazard totem pole. The list forms priorities for allocating funds to correct the hazards. The list can include the cost to correct each hazard and a cumulative cost that sums costs for scenarios starting from the top. Managers have limited resources and are not likely to be able to correct every hazard in the list. They must decide how far down the list they want to go, can afford to go, or both with their budget. At some point there is a cutoff. Funds will not support items below the cutoff line.

The items that are funded are converted to an action plan for implementing the corrections. The process is repeated periodically to identify new scenarios and hazards, and as a result, there is a new funding consideration list for management.

36-7 MANAGEMENT OVERSIGHT AND RISK TREE

Another method that is a derivative of system safety and fault tree analysis techniques is management oversight and risk tree (MORT), which is both a program and a logic diagram. As a program, MORT helps prevent safety-related oversights, errors, and omissions, and it attempts to identify and assess risks associated with an operation and refer them to the proper management level for action. MORT programs help optimize allocation of funds for safety programs and hazard control. MORT incorporates behavioral, organizational, and analytical sciences in dealing with energy transfer, error, change, and risk in a systematic way.

As a diagram, MORT arranges safety program elements in an orderly and logical manner. MORT diagrams structure safety literature and practices into three levels of relationships. At the top level, MORT identifies 98 generic problems or *undesirable events*. At the second level, there are 1,500 possible causes, termed *basic events*, for these problems. At the third level, there are thousands of *criteria* (standards, codes, practices, etc.) to judge whether steps in a safety program are done well or are less than adequate (denoted by LTA).

MORT can be used to investigate accidents or evaluate safety programs. A MORT diagram is an idealized safety system model that uses the logic of fault tree analysis. MORT assumes that in a *perfect* safety system, all components function in a manner that contributes to or complements the achievement of tasks. A safety system or program is a process of eliminating or controlling hazardous events through engineering, design, education, management policy, and supervisory control of conditions and practices.

The general features of a MORT event tree are shown in Figure 36-9. This example gives a general flavor for MORT diagrams and analysis. There are many rules and procedures that cannot be covered here that make MORT an effective tool. In a MORT diagram, generic events are at the top. At the second tier are specific or management oversights and omissions and assumed risks (denoted by R). Specific (denoted by S) refers to events or factors that are specific to an accident. Management (denoted by M) refers to factors in the general management system or context. At the lower tiers, basic events and contributing factors and controls that failed are detailed.

36-8 OTHER ANALYSES AND APPLICATIONS OF SYSTEM SAFETY

There are several other extensions of system safety analysis and techniques that make the system safety approach an effective one. Applications of system safety methods, often with some variance from more formal procedures, have found their way into dealing with many safety problems.

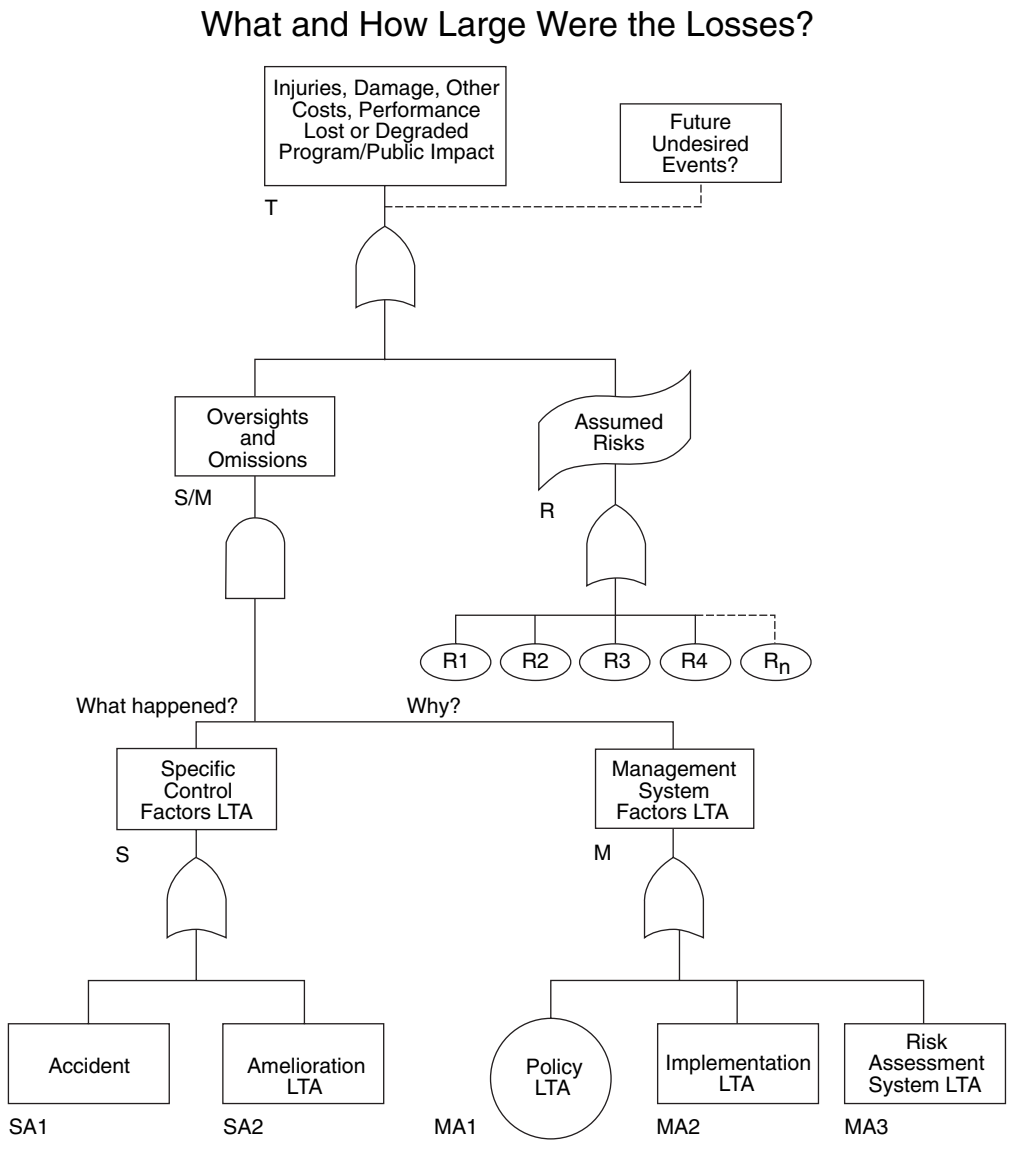

Figure 36-9. An example of the top portion of a MORT diagram. (From *MORT Users' Manual*, Revision 2, DOE 76-45/4, SSDC-4, U.S. Department of Energy, Washington, DC, May, 1983.)

Energy Analysis

For many safety problems, an analysis of energy in various forms, transfer of energy, and release of energy is very useful. Haddon's theories about energy and control of it (see Chapter 3) are a significant part of energy analysis. When analyzing machines, equipment, processes, and operations, an analysis of energy can identify many hazards that need to be controlled. Figure 36-10 is an incomplete diagram of several forms of energy that might be considered during an energy analysis.

For example, a punch press has energy in the moving flywheel. During the machine operation, the energy is transferred to the action of the punch. There are dangers associ-

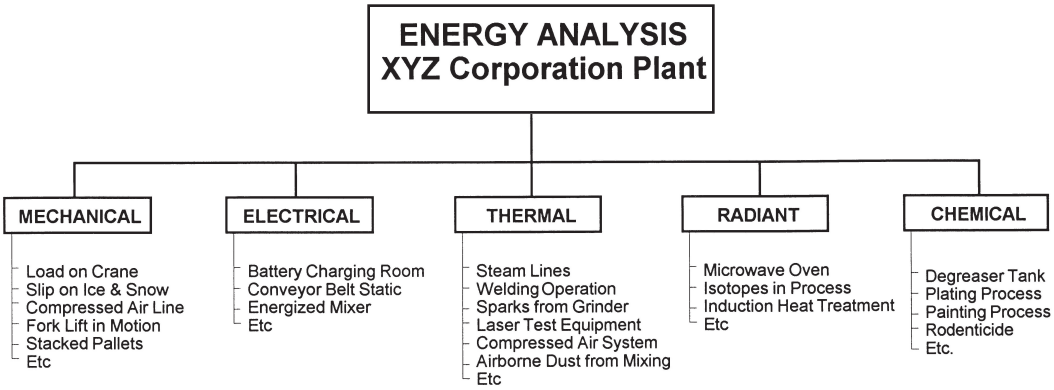

Figure 36-10. Example of an energy analysis chart.

ated with the flywheel and the punch actions that need protection. In addition, there are springs that store energy in the die or elsewhere. Parts of the machine are held in place by brakes during idle phases of the punch cycle. A failure of the brake could release potential energy in the weight of the elevated components and the parts could fall. Similarly, energy could be released while dies are changed. Thus, a die prop is needed to prevent potential energy from becoming kinetic energy. A motor in the press has electrical energy that is converted to mechanical energy. Unprotected electrical energy could lead to injury directly or through its transfer at the wrong time to the machine components.

Energy analysis may be helpful in identifying risks in powered systems and equipment and in establishing engineering and administrative controls as well as lock-out and tag-out procedures.

Buildings

The Department of Defense may require that system safety be applied to construction projects. At minimum, a preliminary hazard analysis must be performed for the facility, its subsystems, and use during its planning and early design. Depending on results, further analysis may be needed to identify further hazards and suitable controls for the building life cycle. The U.S. Army Corps of Engineers developed a procedural guide for applying system safety to building projects.[5]

Fire Safety

The National Fire Protection Association (NFPA) recognized that a building and its fire safety could benefit from a systems analysis. A structure is a system made up of many components. Buildings and structures are modified over time and their conditions often change. Codes and standards for fire safety also change with time. A systems approach for analyzing the fire safety of a building can help identify deficiencies and pinpoint corrective actions.

NFPA has developed a fire safety concepts tree.[6] At the top of the tree is fire safety objective(s), followed by actions to achieve the objectives. Elements of the tree are connected by AND and OR gates, similar to fault tree analysis. Figure 36-11 illustrates the upper levels of the tree. The tree is useful in building analysis and design and can be used for qualitative and quantitative analysis.

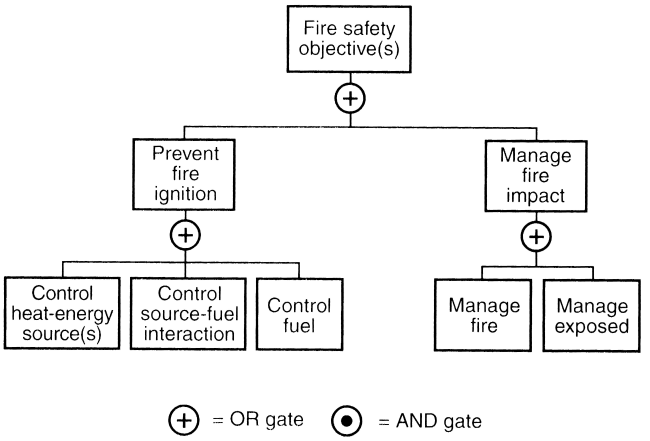

Figure 36-11. Upper levels of the fire safety concepts tree. (Reprinted with permission from the *Fire Protection Handbook*, 19th ed., 2003, National Fire Protection Association, Quincy, MA, 02169.)

EXERCISES

1. The circuit, fault tree, and probabilities of events in the fault tree are shown in Figure 36-12.
   (a) Compute the failure rates for branches (a) and (b).
   (b) Compute the failure rate for the top event.
   (c) Which branch is more critical (more likely to cause failure)?
   (d) Which failure or fault is most likely to cause the system to fail?
2. Obtain a copy of a fault tree analysis for a system and review the analysis and results. You may wish to look at one of the classic reports on nuclear power plant safety: *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*, Report WASH-1400, U.S. Nuclear Regulatory Commission, October 1975. (This report is also known as the Rasmussen report.)

REVIEW QUESTIONS

1. What is system safety?
2. Where did system safety originate?
3. What military standard documents the general procedures for system safety?
4. Briefly explain a system safety program and its objectives.
5. List five system safety design requirements.
6. Identify the precedence for meeting system safety requirements.
7. What are the two classes of system safety tasks? Identify five tasks within each class.
8. What does PHA stand for?
9. What is fault tree analysis? For what is this method used to analyze?
10. What are three limitations of fault tree analysis?

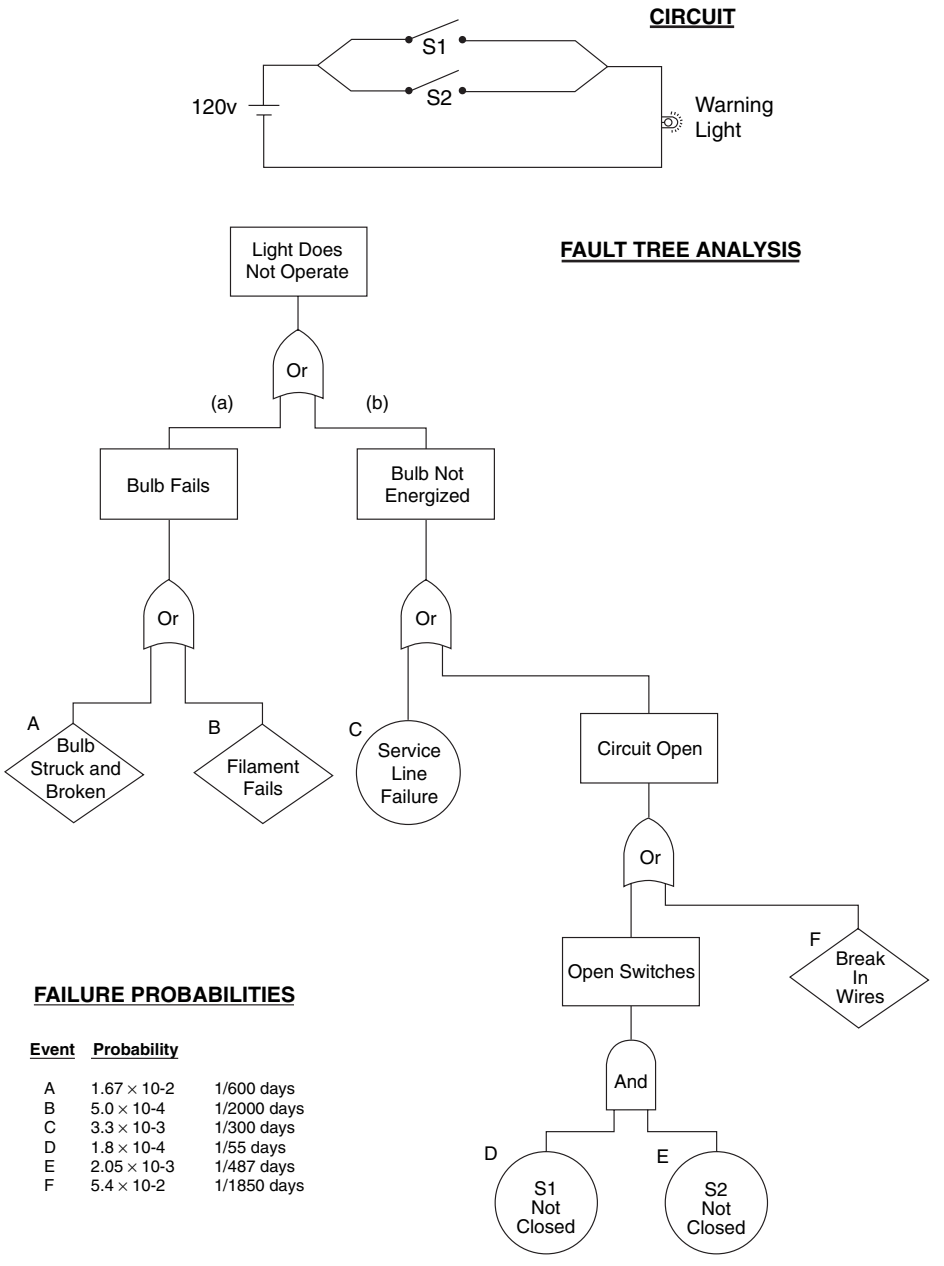

Figure 36-12. System and fault tree diagrams for Exercise 1.

11. What symbols are used in fault tree analysis to represent each of the following factors?

(a) a basic event

(b) an undeveloped event

(c) a normal event

(d) AND logic gate

(e) OR logic gate

(f) inhibit logic gate

(g) a transfer or discontinuity in a fault tree diagram

12. What is the difference between a fault and a failure?

13. What are the four classes of causal events in fault trees?

14. What kinds of analyses can be performed on a fault tree?

15. What is a cut set?

16. What is FMEA? For what is this method used to analyze?

17. What is STEP analysis? For what is this method used to analyze?

18. What is the hazard totem pole? Explain how is it used.

19. What is MORT? What is this method used for?

NOTES

1 29 CFR 1910.119, Process Safety Management of Highly Hazardous Chemicals.

2 *System Safety Analysis Handbook*, 2nd ed., System Safety Society, Unionville, VA, 1997.

3 Recht, J. L., "Systems Safety Analysis: The Fault Tree," *National Safety News*, 93:37–40 (1966).

4 Grose, V. L., *Managing Risk: Systematic Loss Prevention for Executives*, Prentice-Hall, Englewood Cliffs, NJ, 1988.

5 *Facility System Safety Program Manual*, HNDP 385-3-1, U.S. Army Corps of Engineers, Huntsville Division, Huntsville, AL, October, 1985.

6 *Fire Protection Handbook*, 19th ed., National Fire Protection Association, Quincy, MA, 2003.

BIBLIOGRAPHY

BROWN, D. B., *Systems Analysis and Design for Safety*, Prentice-Hall, Englewood Cliffs, NJ, 1976.

DAUGHERTY, E. M., Jr., and Fragola, J. R., *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, Wiley, New York, 1984.

GREEN, A. E., *Safety Systems Reliability*, Wiley, New York, 1984.

HAMMER, W., *Handbook of System and Product Safety*, Prentice-Hall, Englewood Cliffs, NJ, 1972.

HENLEY, E. J., and Kinamoto, H., *Designing for Reliability and Safety Control*, Prentice-Hall, Englewood Cliffs, NJ, 1985.

JOHNSON, W. G., *MORT Safety Assurance Systems*, Marcel Dekker, New York, 1980.

LEVESON, NANCY G., *Safeware—System Safety and Computers*, Addison-Wesley, Reading, MA, 1995.

MALASKY, S. W., *System Safety: Technology and Application*, 2nd ed., Garland STPM Press, 1982.

PERROW, C., *Normal Accidents: Living with High-Risk Technology*, Basic Books, Inc., New York, 1985.

RAHEJA, DEV G., *Assurance Technologies—Principles and Practices*, McGraw-Hill, New York, 1991.

ROLAND, H. E., and Moriarity, B., *System Safety Engineering and Management*, 2nd ed., John Wiley & Sons, New York, 1990.

Standard Practice for System Safety, Military Standard MIL-STD-882D, U.S. Department of Defense, Washington, DC, February 10, 2000.

STEPHANS, RICHARD A., *System Safety for the 21st Century—The Updated and Revised Edition of System Safety 2000*, John Wiley & Sons, New York, 2004.

STEPHANS, RICHARD A., and Talso, Warner W., *System Safety Analysis Handbook*, System Safety Society, Unionville, VA, 1997.

STEPHENSON, JOE, *System Safety 2000—A Practical Guide for Planning, Managing, and Conducting System Safety Programs*, Van Nostrand Reinhold, New York, 1991.

VINCOLI, JEFFREY W., *Basic Guide to System Safety*, Van Nostrand Reinhold, New York, 1993.