

program development and adaptation to local needs and resources are compiled;

3. The bimodal simulator that is to be used for training drivers in key collision-avoidance skills should be defined, developed, and preliminarily tested;

4. The method for in-vehicle training in collision-avoidance techniques that satisfies requirements for safety, reality, low cost, and training staff situation control (the advanced driving range concept) should be defined; and

5. The research problems that must be addressed before an accident-avoidance, skill-training program can become a reality should be identified and, if possible, resolved.

The principal conclusion reached during this program is that accident-avoidance skill training is necessary, is feasible, and can be accomplished at a reasonable cost. The products of this study, in both phases 1 and 2, are believed to provide the basis for continuation of this development program area under the continuing sponsorship of the National Highway Traffic Safety Administration.

ACKNOWLEDGMENTS

This project was supported by the National Highway Traffic Safety Administration. All conclusions and recommendations are our responsibility.

Special appreciation must be expressed for the guidance and patience of Herbert R. Miller, who was the contract technical manager for this study and without whom the results achieved would not have been possible.

We also wish to acknowledge the contributions of James R. Bathurst, who conceived and developed the bimodal simulator and the advanced driving range training concepts; A. James McKnight, who directed the portion of the study accomplished by Central Missouri State University; and Ronald W. Drahos and John R. Treat, who directed the accident data analysis performed by the Institute for Research in Public Safety of Indiana University.

REFERENCES

1. Workshop on Advanced Driver Education Techniques. Proc., Office of Driver Performance Research, National Highway Traffic Safety Administration, Jan. 21, 1972.

2. An Analysis of Emergency Situations, Maneuvers, and Driver Behaviors in Accident Avoidance. Institute for Research in Public Safety, Indiana Univ., Final Rept., Feb. 14, 1975.
3. Collision Avoidance Training: Analysis of Requirements Imposed Upon Drivers by Collision Avoidance Situations. National Public Services Research Institute, Central Missouri State Univ., Final Rept., Feb. 1975.
4. G. R. Hatterick. Preliminary Curriculum and Performance Measurement Specification for Accident Avoidance Skill Training and Performance Testing. URS/Matrix Co., Falls Church, Va., Rept. PR-0530-19, Sept. 12, 1975.
5. Tri-level Study of the Causes of Traffic Accidents. Institute for Research in Public Safety, Indiana Univ.; National Highway Traffic Safety Administration, Repts. DOT-HS-801-334 and DOT-HS-801-335, Vols. 1 and 2, Aug. 1973.
6. Tri-level Study of the Causes of Traffic Accidents. Institute for Research in Public Safety, Indiana Univ.; National Highway Traffic Safety Administration, Interim Rept. 2, Vols. 1, 2, and 3, June 1975.
7. G. R. Hatterick and J. R. Bathurst. Accident Avoidance Skill Training and Performance Testing. URS/Matrix Co., Falls Church, Va., Final Rept; National Highway Traffic Safety Administration, Rept. DOT-HS-801-852, March 1976.
8. C. O. Hopkins. How Much Should You Pay for That Box? Human Factors, Vol. 17, No. 6, Dec. 1975.
9. A. J. McKnight and others. Driver Education Task Analysis. Human Resources Research Organization, Alexandria, Va., Vols. 1, 2, 3, and 4, 1970.
10. Accident Facts. National Safety Council, 1975.
11. Accident Facts. National Safety Council, 1974.
12. R. F. Pain. Accident Avoidance Skill Training and Performance Testing. URS/Matrix Co., Falls Church, Va., Rept. PR-0530-09, April 1975; National Highway Traffic Safety Administration.

Publication of this paper sponsored by Committee on Driver Education.

**Messrs. Hatterick and Pain were with URS/Matrix Company, Falls Church, Virginia, when this research was performed.*

System-Safety Techniques Useful for Transportation Safety

Michael Horodniceanu, Edmund J. Cantilli, Martin L. Shooman, and Louis J. Pignataro, Department of Transportation Planning and Engineering, Polytechnic Institute of New York

This paper reviews existing system-safety techniques in terms of their applicability to the current transportation structure, status, and available data; their ease of comprehension; and their usefulness in reducing accidents and fatalities. The two techniques of failure mode effects and criticality analysis and fault-tree analysis are reviewed, explained, and modified for use in transportation safety studies. When applied at each level or activity cycle of a transportation system, these

two techniques provide safety specialists with tools that lead to concern for safety at every stage of a project from conception through facility operation. The cohesive approach that is suggested by the concept of system safety is well-suited to the needs of transportation safety. As a methodology, system safety must be adopted and its technical and managerial analyses applied at the modal facility level.

Currently, transportation safety is a field of activity in disparate parts, many of which are not necessarily interrelated, interdependent, or mutually helpful for cohesively tying transportation safety efforts. The integration of all safety-related activities is facilitated by using the systematic, technical-managerial approach to safety that is known as system safety. This approach was initially developed by the military (1, 2) and National Aeronautics and Space Administration (NASA) (3), and is currently being proposed for adoption by the transportation industry.

The system-safety approach is intended to regularize and order safety considerations from the earliest stages of concept formulation through design, testing and evaluation, construction, training, certification, and operation and maintenance. System safety is derived from system-analysis techniques that have been devised and used over the years to maximize system design and operating objectives. The intended use of these techniques has been to enable decision makers to reach correct conclusions by using an orderly process of data collection, modeling, analysis management, and evaluation.

System-safety procedures require a logical examination of all elements of a system, i.e., identifying all possible sources of accidents. The analysis does not end with the identification of system failures; it estimates the probability of accident occurrence and points out the options available for eliminating these occurrences. In addition to safety analysis, system safety includes a set of managerial, contractual, manufacturing, testing, and operational procedures that help improve the decision-making process regarding the elimination of failures. Thus, the need to identify, at the earliest stages of design, all possible elements of combinations of causes that might contribute to a failure of the system led to the development of a set of formalized procedures (system safety) for safety analysis. Terms like safety systems and combinations thereof are frequently used out of context or are referred to from different points of view. For uniformity, these terms are clarified and defined as follows:

1. Safety is freedom from those conditions that can cause injury or death to personnel, or damage to or loss of equipment or property;
2. A system is a composite of controlling contingencies at any level of complexity of operational and support equipment, personnel, hardware and software, and procedures that, used as an entity, are capable of performing or supporting an operational role;
3. A system-safety methodology is a repertoire of tools and techniques that are used to obtain an optimum degree of safety within the constraints of operational effectiveness, time, and cost; and
4. The state of the system is attained through specific application of system-safety management and engineering principles throughout all phases of system-activity cycles (Figure 1).

TRANSPORTATION PROGRAM FOR SYSTEM SAFETY

A transportation program for system safety should follow the phases of the transportation-activity cycle (TAC). First, there is a concept formulation stage, which is the planning period for determining the location of a transportation facility, its characteristics and mode, and its capacity and purpose. This stage is followed by a preliminary design in which alignments may be set and some details of the design and capability are set. The engineering design is the stage in which all details are set down. Production or construction may

involve the guideway or the vehicles of a given system, and, finally, operation, and maintenance represent the ongoing phase of a transportation facility.

In the military and NASA, disposal of an entire system is a distinct phase in the life cycle of a weapons system or a space program; but, in public or private transportation, it is rare that an entire system is disposed of. Generally, the systems are phased and replaced. At any rate, feedback from each phase, and especially from the operating phase, to the planning or conceptual phase is essential to improving the existing and future systems.

The primary function of such a program is to assist management in their attempt to achieve the basic safety goals and objectives of the system. The preparation of a transportation system-safety program plan (TSSPP) is the backbone of a systematic approach to the problem. The development of such a plan is usually divided into two basic phases: (a) preparation of a preliminary TSSPP and (b) preparation of a final TSSPP.

The preliminary phase is primarily a managerial tool for setting forth the safety-planning procedures. The following are some of the basic points to be developed under such a management plan:

1. Define the system;
2. Set safety goals and objectives;
3. Determine organizational structure and responsibilities;
4. Identify, in preliminary fashion, the hazards and how to control them;
5. Define and describe scheduling and review procedures (establish milestones);
6. Describe methods for evaluating and monitoring performance; and
7. Define data base and documentation requirements and procedures.

The system definition should not be limited only to central elements, but should also include an identification and definition of subsystems and internal and external elements that might have an effect on the system.

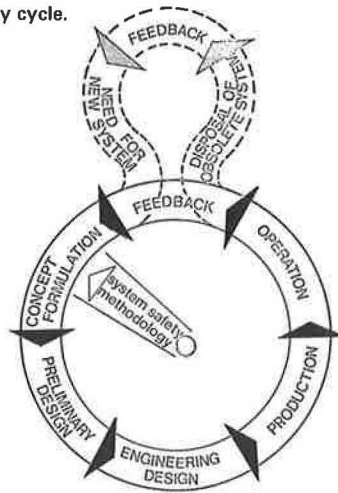
Specific safety goals and objectives should be established to give a safety program a definite direction. These objectives should cover both short- and long-range goals. Some questions that must be posed and answered at this level are as follows: What level of safety is acceptable, and what level of safety is achievable within the given constraints?

Since safety is sometimes overlooked or treated only as an afterthought, sufficient managerial visibility on the topic is a must. This visibility will ensure that the next step is to determine the optimum location of the safety group within the organizational structure and to select and designate qualified personnel by assigning responsibilities respectively.

In addition to having knowledge about the system, the analyst should enter into a preliminary hazard analysis. The purpose of such an analysis is to help develop design requirements that are used in the conceptual phases of system development. Data and experience acquired from older, analogous systems should also be employed in determining preliminary hazards. Milestones should also be established to ensure effective and timely review and modification of the system-safety objectives. Milestones are formally designated points in a program that are chosen because of their prominent significance. Usually, milestones are identified as crucial points in a program where progress is assessed and decisions are made.

A description of methods to be used for the purposes of evaluating and monitoring the effectiveness and per-

Figure 1. Transportation-activity cycle.



formance of the program should follow. A data base should be established, and procedures for data collection and analysis should be defined. A preliminary system-safety program plan also uses elements of program management to ensure the accomplishment of the systems safety tasks. These tasks include identification of the system-safety requirements and planning and organization of the efforts directed toward the safety objectives.

Thus, the final version of the TSSPP is a document with a technical and engineering content that is more developed than in the preliminary TSSPP. A checklist of requirements for a system-safety program, as used in the military and industry (4, 5), is as follows:

1. Purpose and scope
2. Applicable documents (only documents cited in the plan text)
3. Safety organization
 - a. Relation to total organization
 - b. Organizational array
 - c. Responsibilities
 - d. Interfaces
4. Safety tasks to be completed
 - a. Criteria development
 - b. Analyses
 - c. Design (program review participation)
 - d. Contractor (subcontractor requirements)
 - e. Reporting
 - f. Documentation
 - g. Planning
 - h. Evaluations
5. Methods for accomplishing safety tasks
 - a. Criteria development, documentation, and monitoring
 - b. Analysis technique
 - c. Other program activities
6. Schedule for task completion (keyed to major program milestones)

The evaluation of the safety program should be performed to assure compatibility with stated goals and objectives. Sometimes such assessments may lead to realignment of the program or redefinition of the goals.

Once the boundaries of the system have been defined, possible hazards identified, and objectives established, analytical techniques are employed to analyze the system and data regarding failure roles, repair roles, and probabilities and environmental conditions collected for the analysis. There are many analytical techniques available for hazard and risk evaluation and some of these include failure mode effects and criticality analysis (FMECA), fault-tree analysis (FTA), reliability analysis, risk analysis, procedure analysis, human factors analysis, and task analysis.

ANALYTICAL SAFETY TECHNIQUES

The analytical techniques described below should be used in the early stages of the system-development process (even if they are based on scant information) and updated at key milestones when further details and data become available. Although several techniques were previously mentioned, the purpose of this paper is to illustrate and analyze the merits and demerits of two analytical techniques that lend themselves to the analysis of safety-related problems: FMECA and FTA (6, 7).

Failure Mode Effects and Criticality Analysis

Failures can be classified in many ways, depending on the specific object of the analysis. In some instances, failures are classified according to reparability or repair time; in other instances, they are classified according to the severity of effect on safety in a system (e.g., whether the result is a fatality or an injury). Different failure modes arise through different failure mechanisms that exhibit different characteristics; consequently, different types of corrective actions are required to minimize the probability and severity of an accident. Thus, it is implied that a component may exhibit several different failure modes in that each mode is characterized by its own failure rate and set of failure mechanisms; therefore, each failure should be considered individually, and all consequences of the given failure should be analyzed accordingly.

At an early stage in system development, when only the broad concepts of system operation are known, the concept of failure modes allows for the performance of a safety analysis, which provides a basis for later studies.

FMECA is initially constructed and periodically updated to reflect changes and improvement in design and application. These steps are necessary for evaluating the various alternatives during the early design stages. FMECA should be performed or updated at the following major milestones:

1. Concepts formulated and alternatives selected,
2. Preliminary design and planning of system completed,
3. Detailed subsystem designs completed, and
4. Design improvements introduced.

The basic questions to be answered in FMECA are as follows:

1. How can each component conceivably fail?
2. What mechanisms might produce these modes of failure?
3. If a failure does occur, what could be the effects?
4. What is the severity (criticality) associated with a given failure?

Once the analysis is completed, it will shed light on two important aspects: (a) the manner in which the failures can be detected, and (b) the existence of inherent provisions in the system to compensate for the effects of a failure.

Before an actual FMECA is performed, the following preparatory steps are required.

1. Define the system, its boundaries, and its mission(s);
2. Describe the operation of the system;
3. Identify failure categories; and
4. Describe the environmental conditions.

The degree to which the preparatory steps are performed depends on the complexity of the system that is being studied and the experience that one has with similar systems. The more complex the system, the greater the need to carefully define it. The original FMECA was extended to suit various applications, and the modifications are reflected in the titles. However, the fundamental technique remains unchanged. The following information is required for performing FMECA:

1. Functional diagrams, schematics, and drawings of each subsystem for facilitating the determination of interrelations;
2. A complete list of components in each subsystem and the specific function of each component;
3. The establishment and review of operational and environmental stresses that affect the system for determining the effects on the system or the components; and
4. The identification of significant failure mechanisms that could occur by using historical data on types of failures for different systems and subsystems.

Although this method is simple and direct in its approach to safety-related problems, it also has limitations. The most obvious and serious problem in this method is that the analyst is unable to find possible system failures caused by a combination of failures of individual components because none would have been considered hazardous by itself. Since this method was previously developed for hardware analysis, the combined effect of a component failure factor, which is not hazardous by itself, and the factors of adverse environmental conditions and human errors, which may lead to the creation of a serious system failure, may also be omitted in the consideration. Therefore, FMECA was improved and made acceptable for broader use by introducing a human error factor. Thus, the accident cause-consequence analysis (ACCA) is used. This method provides a step-by-step procedure for listing all hardware failures, human errors, adverse environmental conditions, and procedural incompatibilities that may lead to an unsafe state in the system.

The proposed column headings with subheadings for an ACCA form are as follows:

1. Specific operation or work task
2. Source of hazard
3. Basic causes
 - a. Mechanical failure
 - b. Human error
 - c. Procedural incompatibility
 - d. Adverse environmental condition
4. Possible consequences
 - a. Direct

- b. Indirect
- c. Ultimate to the system

5. Severity
6. Probability of occurrence
7. Suggested preventive and control action

- a. Hardware
- b. Human error
- c. Procedural incompatibility
- d. Adverse environment condition

8. Estimated rate of return

A carefully conducted ACCA is useful because it forces the identification of possible failures, which provides invaluable inputs to FTA.

Fault-Tree Analysis

Fault-tree analysis is a technique that uses logic diagrams to represent and record a deductive reasoning process (9). Although relatively new, the technique lends itself to application in various fields and can successfully be used at all levels of complexity. Similar to other techniques, FTA uses certain symbols and notations (Figure 2).

The foundation of a fault tree is the notion of logic gates, which was borrowed from the field of electrical engineering. The gates indicate whether a single event or a combination of events is required to produce the next level of events. Only two types of gates are necessary, AND gate and OR gate, to perform a fault-tree analysis.

1. The AND gate is defined as a logical operation that produces an output event requiring the coexistence of all the input events. In set theory, this gate is referred to as an intersection.

2. The OR gate is defined as a logical operation that produces an output event if one or more of the input events exist. In set theory, this gate is referred to as a union. It should also be noted that there can be no fewer than two inputs to this gate.

Any other logic gates are only special combinations or modifications of the fundamental gates, and these would be created for purposes of convenience. A fault tree can be constructed by using only the fundamental gates. The concept of negation or NOT (called complement inset theory) is also needed. For example, if the brakes on a car working is denoted by BGood, then the event in which the brakes are not working is denoted by NBGood.

In the process of constructing a fault tree, the analyst should distinguish between two basic types of events.

1. Desired events are those events that take place in a normal and planned change of state, and
2. Undesired events are those events that take place in an abnormal and unwanted change of state.

Undesired events can further be divided into independent and dependent events as follows:

1. An independent event can be defined as an event that does not depend on other components in the system for its occurrence. It is a single element in a dynamic change of state from an unfailed state. Frequently, an independent event will also be defined as a basic fault event.

2. A dependent event is the resultant output event of a logic gate. It is dependent on the type of logic gate

Figure 2. Description of fault-tree symbols.

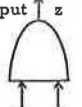

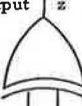


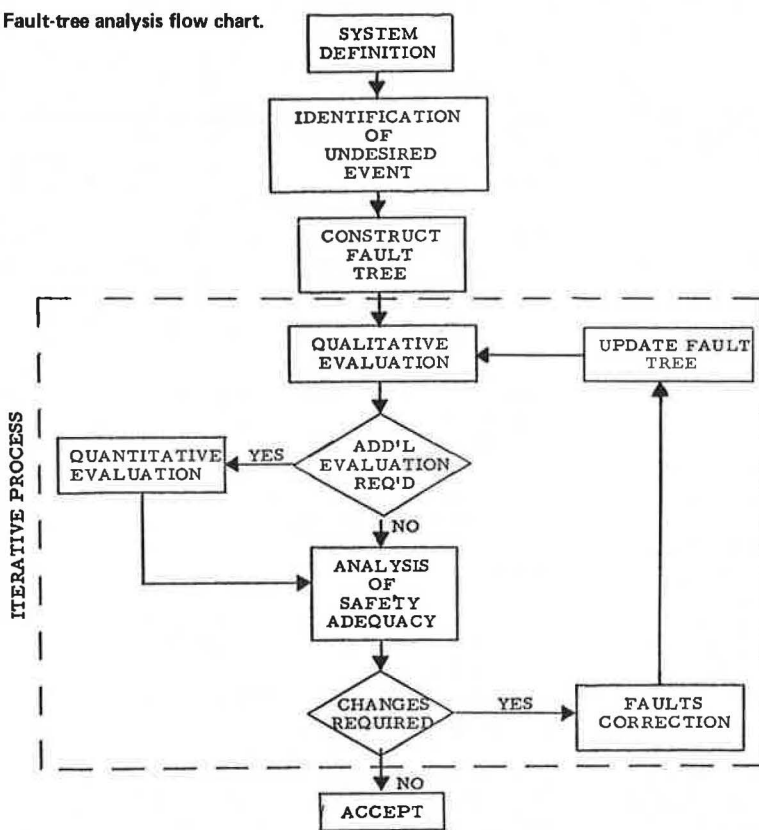
Logic Gate and Mathematical Symbols	Terminology	Relation Between Input and Output	Truth Table 1 ≡ occurrence of the event 0 ≡ absence of the event																		
 <p>output ↑ z Inputs x y $Z = X \cap Y$</p>	'AND' Gate Intersection	$z = (x) \text{ and } (y)$	<table border="1"> <thead> <tr> <th colspan="2">Inputs</th> <th>Outputs</th> </tr> <tr> <th>x</th> <th>y</th> <th>z</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>0</td></tr> <tr><td>0</td><td>1</td><td>0</td></tr> <tr><td>1</td><td>1</td><td>1</td></tr> </tbody> </table>	Inputs		Outputs	x	y	z	0	0	0	1	0	0	0	1	0	1	1	1
Inputs		Outputs																			
x	y	z																			
0	0	0																			
1	0	0																			
0	1	0																			
1	1	1																			
 <p>output ↑ z Inputs x y $Z = X \cup Y$</p>	'OR' Gate Union	$z = (x) \text{ or } (y)$	<table border="1"> <thead> <tr> <th colspan="2">Inputs</th> <th>Outputs</th> </tr> <tr> <th>x</th> <th>y</th> <th>z</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>1</td><td>1</td></tr> </tbody> </table>	Inputs		Outputs	x	y	z	0	0	0	1	0	1	0	1	1	1	1	1
Inputs		Outputs																			
x	y	z																			
0	0	0																			
1	0	1																			
0	1	1																			
1	1	1																			
 <p>output ↑ z Inputs x y $Z = (X \cap \bar{Y}) \cup (\bar{X} \cap Y)$</p>	'Exclusive or' Gate	$z = \{(x) \text{ and } (\text{not } y)\} \text{ or } \{(\text{not } x) \text{ and } (y)\}$	<table border="1"> <thead> <tr> <th colspan="2">Inputs</th> <th>Outputs</th> </tr> <tr> <th>x</th> <th>y</th> <th>z</th> </tr> </thead> <tbody> <tr><td>0</td><td>0</td><td>0</td></tr> <tr><td>1</td><td>0</td><td>1</td></tr> <tr><td>0</td><td>1</td><td>1</td></tr> <tr><td>1</td><td>1</td><td>0</td></tr> </tbody> </table>	Inputs		Outputs	x	y	z	0	0	0	1	0	1	0	1	1	1	1	0
Inputs		Outputs																			
x	y	z																			
0	0	0																			
1	0	1																			
0	1	1																			
1	1	0																			
	'Intermediate Dependent Event'	-----	-----																		
	'Independent (Basic) Event' Sometimes Called a 'Basic Fault'	-----	-----																		

Figure 3. Fault-tree analysis flow chart.



employed and the input events to the logic gate. Dependent events are also called gate fault events. During fault-tree development, the gate fault events on one level may become input events to gate fault events on higher levels.

Thus, FTA as used in a system-safety program involves several basic steps (Figure 3).

The analysis is started by first defining the system under investigation. For the conclusions to be meaningful, a system reference line should also be included. This is also the stage in which the researcher will define the constraints (limits) to be placed in terms of time, cost, results desired, and such. The next step is to determine the top undesired event. The definition of this event is dependent on the needs, requirements, and objectives of the program under consideration. After defining the event to be analyzed, the building of the fault tree begins. The deductive process starts with the development of cause and effect relations of faults and normal events throughout the system. This process involves determining the type of gates and inputs to these gates at each level of the fault tree. The adequacy of the construction is dependent on the amount and quality of information and the data and knowledge acquired about the system.

Following the definition of the system and the identification of the top undesired event, other potential accidents and hazardous conditions related to the system are also identified and structured into a top event or tree-top event. The top event is used to identify those areas that need to be developed or expanded by further analysis. An important step in the construction of fault trees is dividing the tree events into phases that correspond to the system-operating phases. This second level of fault-tree development is done by examining the system elements from a functional point of view. Fault-tree development continues with the identification of normal and fault events in the system, until all events are definable in terms of basic events for which failure rates or estimates become available.

Once the fault-tree structure is complete, an evaluation is performed. The purpose of the evaluation is to determine what risks are associated with the top undesired event and which ones are unacceptable and require elimination.

The evaluation may be done on two levels.

1. The qualitative evaluation is an inspection or an engineering judgment; the fault tree is mainly used as a visual aid to clarify relations.
2. The quantitative evaluation is one in which known failure rates of the system elements are used and combined to yield a numerical evaluation of the undesired event.

The information acquired through the qualitative and quantitative analyses is then used to analyze the safety of the given system. If the problem areas are identified and found unacceptable, corrective action is taken and the fault-tree structure or failure rules are changed to correspond to the modified system. The process is reiterated until the system is safe for acceptance.

The qualitative analysis of a fault tree implies that the analyst will have a thorough familiarity with the system under investigation. This analysis will generally proceed from top to bottom. Occasionally, it is convenient to check or construct some paths by working from bottom to top. At each OR gate, the analyst will have to decide, on the basis of his or her knowledge and experience, which paths to follow, thus indicating the most likely path to lead to the event above the OR gate.

The process is repeated for every branch until each path terminates in basic fault events. The analyst will then determine the most likely path of events leading to the top undesired event. The outcomes of such a qualitative evaluation are not as manageable as the quantitative ones, but sometimes the qualitative evaluation includes practical considerations that are not easily quantifiable.

If more information is required, a quantitative evaluation of a fault tree is started. The following four basic steps are involved in the quantitative evaluation:

1. Convert logic diagram into a mathematical expression,
2. Eliminate all redundancies,
3. Compute probabilities of top undesired events, and
4. Determine criticality of input events.

The logic diagram is converted into algebraic form by using elements of set theory and Boolean algebra. Figure 4 shows the different relations by using the mathematical laws applicable to Boolean algebra and set theory. The quantitative evaluation of a fault tree is possible only when data for the occurrence probabilities of the basic failure events are available. Four basic results are obtained from a numerical evaluation of the fault-tree equations:

1. The probability of occurrence of the undesired event,
2. The importance of the undesired event,
3. The importance of the various paths leading to the undesired event, and
4. The establishment of a reference level of safety to be used in determining effectiveness of changes.

In preparing a fault-tree diagram, only those elements that contribute to the occurrence of an undesired event should be considered. Therefore, the effort is directed toward the study and control of safety-related problem areas. The importance of an undesired event is a function of the effect it has on overall system safety and its frequency of occurrence. The undesired event that results in a fatality may be considered most critical, while the undesired event that causes minor injury may be considered the least critical. These factors must also be taken into consideration in safety analysis. The utility of the fault-tree analysis technique is found in the orderly and concise manner by which it identifies potential problem areas and reveals their impact on the system.

The use of both ACCA and FTA is illustrated by investigating a situation in which there is need for an emergency deceleration. The automobile used in the example is a 1969 Ford. The testing automobile does not have power or antiskid brakes, a parking brake, or dashboard warning lights.

An example of ACCA for an emergency deceleration is as follows. The specific operation or task is to decelerate a vehicle and come to a full stop. The sources of hazard are

1. Vehicle operator fails to stop automobile;
2. Adverse weather conditions such as skidding and poor visibility;
3. Heavy traffic conditions in which vehicles are tailing each other; and
4. Brake failures in (a) one-half of the system (4.1), (b) total system (4.2), (c) master cylinder for one-half of the system (4.3), (d) master cylinder for total system (4.4), (e) self-adjusting mechanism in the drum brakes (4.5), (f) tubing brackets and con-

Figure 4. Conversion of logic diagrams into algebraic forms.

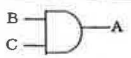
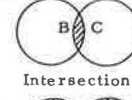
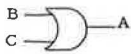
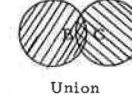

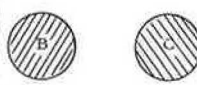
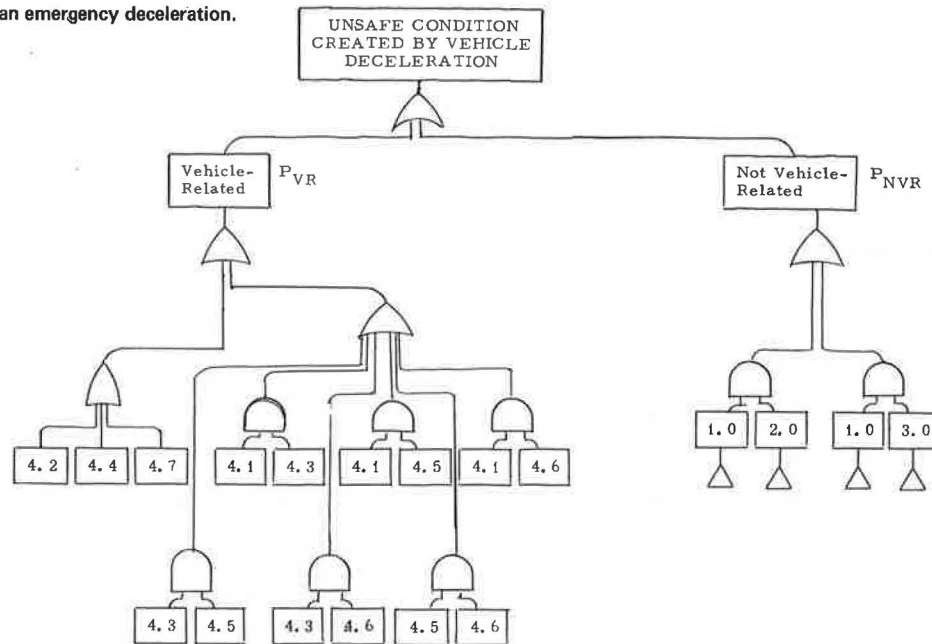
Logic Gate	Venn Diagram	Logic Equation
	 <p>Intersection</p>	$P(A) = P(B) \cdot P(C)$
	 <p>Union</p>	$P(A) = P(B) + P(C)$ $- P(B) \cdot P(C)$
 <p>Special Case of a Disjoint (Mutually Exclusive) Union</p>		<p>Note $P(B) \cdot P(C) = 0$ Therefore $P(A) = P(B) + P(C)$</p>

Figure 5. Fault tree for an emergency deceleration.



nectors (4.6), and (g) pedal and linkage (4.7).

In this case, human error, procedural incompatibility, and adverse environmental conditions are not applicable (basic causes and suggested preventive and control action). However, mechanical failures apply to brakes and include the following for the above mentioned areas: (a) leakage or blockage (4.1, 4.3, 4.6), (b) leakage affecting both front and back systems (4.2, 4.4), (c) leakage or blockage to one wheel only (4.5), and (d) broken or jammed mechanism (4.7).

The direct possible consequences include a reduction in the braking efficiency (4.1, 4.3, 4.6), a loss in the braking system (4.2, 4.4, 4.7), and an imbalance in the brakes that cause the vehicle to behave erratically. The indirect probable causes are that an automobile collides with a moving or standing vehicle(s) or an automobile hits a moving or standing pedestrian. The ultimate possible consequence to the system is damage to the automobile, operator, and occupants; other automobiles and their occupants; and property. The severity is rated moderate (4.1, 4.3, 4.5, 4.6) and high (4.2, 4.4, 4.7). The probability is determined accordingly. For the suggested preventive and control actions, hardware can be adjusted by better maintenance or by better

brakes with an estimated rate of return that is moderate and high respectively.

Thus, it can be seen that a multitude of causes can lead to the creation of a hazardous situation. The analysis is facilitated by using only a simplified braking system. It was determined from inspection that hazards 4.2, 4.4, and 4.7 should be looked at in detail during design review to assure that the probability of a hazard occurring is minimized. The next step in the analysis is to construct a fault tree (Figure 5). The assumptions made were that an unsafe condition occurs if

1. Modes 4.2, 4.4, or 4.7 occur individually;
2. Modes 4.1, 4.3, 4.5, and 4.6 occur in pairs (actually the paired modes must affect both front and rear systems to constitute a failure; therefore, for simplicity, an approximation was made);
3. Modes 1.0 and 2.0 occur in pairs; and
4. Modes 1.0 and 3.0 occur in pairs.

For illustrative purposes only, the probability for the vehicle-related failures (P_{VR}) is computed as follows:

$$P_{VR} = P[(x_{4.2} + x_{4.4} + x_{4.7}) + (x_{4.1} \cdot x_{4.3} + x_{4.1} \cdot x_{4.5} + x_{4.1} \cdot x_{4.6} + x_{4.3} \cdot x_{4.5} + x_{4.3} \cdot x_{4.6} + x_{4.5} \cdot x_{4.6})] \quad (1)$$

Each failure mode has a different probability of occurrence. The analysis is continued by using the failure data on modes 4.1 through 4.7. For example, if the failure rate for 4.7 were λ failure per kilometer (mile), then

$$P = e^{-\lambda M} \quad (2)$$

if mode 4.7 does not occur in M kilometers and

$$P = 1 - e^{-\lambda M} \quad (3)$$

if mode 4.7 does occur in M kilometers.

For completion of the analysis, the failure rate λ_1 is substituted in the equation for P_{vM} , and this substitution will eventually lead to the computation of the probability of the unsafe situation created by the deceleration. Thus, even for a problem this size, the equations will become long and cluttered with many terms. Therefore, computer analysis programs are used to perform the computations in these complex problems.

Some of the difficulties of and solutions to performing fault-tree analysis are listed as follows:

1. The analysis of a large-scale system is complex; therefore, the analyst must be concerned with including all possible (important) events. The analysis can be cross-checked by comparing it with the ACCA and holding design reviews to discuss and check the model.

2. The exact evaluation of the probabilistic equations for any complex problem can tax a digital computer (the number of computations increases roughly as 2^n for n events). Therefore, the solution is to use analytical approximations to simplify the computations.

3. The basic event probabilities are often difficult to obtain but they are needed for computing the safety index. In many cases, these values can be obtained by averaging the opinions of experts (if no data exist) or by making a parametric study.

4. When a fault tree is used to model systems, some of the probabilities become dependent. Therefore, three special cases are indicated. First, if any two events (A and B) are mutually exclusive (they cannot logically occur at the same time), then any OR expression that involves these events must be evaluated [$P(A \cdot B) = 0$ and not $P(A) + P(B)$]. Often, the exclusive OR gate, as described on the checklist of requirements, is used in the fault tree instead of the regular OR gate when this situation occurs. Thus, the exclusive OR gate reminds the analyst (or signals the computer program) to perform this special evaluation. Second, if any two events (A and B) must occur in sequence (e.g., A before B), then the fault-tree diagram must be modified accordingly. One way to modify the diagram is to use a symbol known as the priority gate, which is a special type of AND gate. This symbol reminds the analyst or signals the computer program that a special condition exists. Another way to handle this case is to define a new event such as priority of A before B (PAB) and use a three-input regular AND gate into which A, B, and PAB events can be fed. Third are the cases in which failure of one component weakens other components, and, thus, the probability of failure is increased. In such a case conditional probabilities must be used to evaluate the resulting expressions.

After the probability of occurrence of the top undesired event is established, the criticality of the input events is evaluated, and the events are ranked so that corrective action can be undertaken. The method is flexible and can be used during any phase of system life, i.e., from conception through operation. Similar to other tools, fault trees are a function of the knowledge and imagination of the analyst; they are only as reliable and useful as the information that is fed into them. The fault-tree method is clearly a systematic way of tracing the vulnerable parts of a system. It is a method that has the ability to provide a simple and visible way of supporting managers and engineers in the decision-making process, particularly in regard to risk acceptability and preventive action.

CONCLUSION

Through the use of a systematic approach to safety, potential hazards can be identified before they are activated. The thrust of a system-safety approach is oriented toward action rather than reaction. This orientation is one of the main differences between the conservative approach to system safety and the dynamic approach to system safety discussed above. Accidents can be prevented if the necessary and adequate actions are taken to eliminate and control hazards. A system-safety approach does not imply that that system must be free of risk, but rather that the risks are controlled and made known to management. Thus, the resources needed to design or redesign a transportation system to meet specified risks can be estimated at the outset and refined as the work progresses. Development of data to support managerial decisions may be seen as the real role of system safety.

REFERENCES

1. System Safety Program for Systems and Associated Subsystems and Equipment. Military Standards, No. 882, 1969.
2. System Safety. Air Force Systems Command, U.S. Air Force, Design Handbook, No. 1-6, 4th Ed., 1974.
3. System Safety. National Aeronautics and Space Administration Safety Manual, Vol. 3, 1970.
4. System Safety Engineering. Space and Missiles Organization, U.S. Air Force Systems Command, Manual, 1973.
5. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. U.S. Atomic Energy Commission, Vols. 1-13, Aug. 1974.
6. W. Hammer. Handbook of System and Product Safety. Prentice-Hall, Englewood Cliffs, N.J., 1972.
7. A. Goldsmith. Guide to System Safety Analysis in the Gas Industry. International Telephone and Telegraph Research Institute.
8. C. A. Erickson. System Safety Analytical Technology: Fault-Tree Analysis. The Boeing Co., 1970.
9. H. A. Watson. Minuteman Launch Control System. Bell Telephone Laboratories, 1962.