THE DIGRAPH-FAULT TREE METHODOLOGY
(AND ITS USE IN TRANSPORTATION
RISK ANALYSIS)

BY HOWARD E. LAMBERT
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>i</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>ii</td>
</tr>
<tr>
<td>1.0 INTRODUCTION</td>
<td>1-1</td>
</tr>
<tr>
<td>2.0 DIGRAPH-FAULT TREE METHODOLOGY</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1 Fault Tree Synthesis and Evaluation Scheme</td>
<td>2-2</td>
</tr>
<tr>
<td>2.2 Terminology and Notation</td>
<td>2-4</td>
</tr>
<tr>
<td>2.3 Edge-Dependent Relationships</td>
<td>2-8</td>
</tr>
<tr>
<td>2.4 Unit Model Digraphs</td>
<td>2-8</td>
</tr>
<tr>
<td>2.5 Control Loops</td>
<td>2-10</td>
</tr>
<tr>
<td>2.6 Feedback Loops</td>
<td>2-11</td>
</tr>
<tr>
<td>2.7 Feedforward Loops</td>
<td>2-13</td>
</tr>
<tr>
<td>2.8 System Digraph Construction</td>
<td>2-19</td>
</tr>
<tr>
<td>2.9 Synthesis Algorithm</td>
<td>2-19</td>
</tr>
<tr>
<td>3.0 TRANSPORTATION RISK MODELING</td>
<td>3-1</td>
</tr>
<tr>
<td>4.0 ACCIDENT MODELING AND ANALYSIS FOR THE MARINE MODE</td>
<td>4-1</td>
</tr>
<tr>
<td>5.0 REFERENCES</td>
<td>6-1</td>
</tr>
</tbody>
</table>

APPENDIX A - GLOSSARY OF TERMS USED IN THE LAPP-POWERS' FAULT TREE SYNTHESIS ALGORITHM
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lapp-Powers' Fault Tree Synthesis and Evaluation Scheme</td>
<td>2-3</td>
</tr>
<tr>
<td>2</td>
<td>Gains Between Process Variables</td>
<td>2-6</td>
</tr>
<tr>
<td>3</td>
<td>Mapping for Regulating Control Valve with Gain -1</td>
<td>2-7</td>
</tr>
<tr>
<td>4</td>
<td>Mapping for Quick Closing Control Valve, Gain -10</td>
<td>2-7</td>
</tr>
<tr>
<td>5</td>
<td>Edge Relationships</td>
<td>2-9</td>
</tr>
<tr>
<td>6</td>
<td>Negative Feedback Loop (NFBL)</td>
<td>2-12</td>
</tr>
<tr>
<td>7</td>
<td>Flow Control Negative Feedback Loop</td>
<td>2-14</td>
</tr>
<tr>
<td>8</td>
<td>pH Control Positive Feedback Loop</td>
<td>2-15</td>
</tr>
<tr>
<td>9</td>
<td>Negative Feedforward Loop</td>
<td>2-17</td>
</tr>
<tr>
<td>10</td>
<td>Negative Feedforward Temperature Control</td>
<td>2-18</td>
</tr>
<tr>
<td>11</td>
<td>Mixing Tee Positive Feedforward Loop</td>
<td>2-20</td>
</tr>
<tr>
<td>12</td>
<td>Digraph for Heat Exchanger</td>
<td>2-22</td>
</tr>
<tr>
<td>13</td>
<td>Fault Tree for Heat Exchanger</td>
<td>2-23</td>
</tr>
<tr>
<td>14</td>
<td>Digraph NFBL Control System</td>
<td>2-26</td>
</tr>
<tr>
<td>15</td>
<td>Negative Feedback Loop Operator</td>
<td>2-28</td>
</tr>
<tr>
<td>16</td>
<td>Failure of NFBL for External Moderate Disturbances</td>
<td>2-30</td>
</tr>
<tr>
<td>17</td>
<td>Fault Tree for M3(+1) NFBL Flow Control</td>
<td>2-32</td>
</tr>
<tr>
<td>18</td>
<td>Digraph Negative Feedforward Control Temperature Control System</td>
<td>2-38</td>
</tr>
<tr>
<td>19</td>
<td>Negative Feedforward Temperature Control System Fault Tree</td>
<td>2-39</td>
</tr>
<tr>
<td>20</td>
<td>Negative Feedforward Operator</td>
<td>2-41</td>
</tr>
<tr>
<td>21</td>
<td>General Form of System Digraph for Test Bed</td>
<td>2-42</td>
</tr>
<tr>
<td>22</td>
<td>Dynamics Associated with Gains</td>
<td>2-45</td>
</tr>
<tr>
<td>23</td>
<td>Pressure Tank System</td>
<td>2-46</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>24</td>
<td>Digraph for Pressure Tank Rupture</td>
<td>2-48</td>
</tr>
<tr>
<td>25</td>
<td>Fault Tree for Pressure Tank Rupture</td>
<td>2-49</td>
</tr>
<tr>
<td>26</td>
<td>Lapp-Powers Fault Tree Synthesis Algorithm</td>
<td>2-51</td>
</tr>
<tr>
<td>27</td>
<td>Railroad Terrain</td>
<td>3-4</td>
</tr>
<tr>
<td>28</td>
<td>Feedforward Control to Prevent Derailment</td>
<td>3-5</td>
</tr>
<tr>
<td>29</td>
<td>Conceptual Relationships of Fault Tree Time Considerations</td>
<td>3-7</td>
</tr>
<tr>
<td>30</td>
<td>Boston Harbor</td>
<td>4-2</td>
</tr>
<tr>
<td>31</td>
<td>Concept of Critical Area</td>
<td>4-5</td>
</tr>
<tr>
<td>32</td>
<td>Digraph for Release of LNG in Boston Harbor Due to LNG Tanker-Ship Collision</td>
<td>4-7</td>
</tr>
<tr>
<td>33</td>
<td>Fault Tree for Release of LNG in Boston Harbor Due to LNG-Tanker-Ship Collision</td>
<td>4-11</td>
</tr>
</tbody>
</table>
ABSTRACT

This report describes directed graph (digraph) fault tree methodology, previous applications of this methodology and its use in modeling accidents in transportation systems. The advantages of the digraph fault tree methodology over standard fault tree analysis are that multivalued logic and dynamics can be considered. A description of how the methodology was applied in generating fault trees for (1) collision between an LNG tanker and another vessel in Boston Harbor and (2) derailment of railroads will illustrate these advantages.
ACKNOWLEDGMENTS

The author wishes to thank Drs. Lloyd Philipson and Harold Roland at the Institute of Safety and Systems Management, University of Southern California for their guidance to the author concerning the modeling of transportation systems. In addition, the author wishes to thank Mr. Colin Dunglinson, a process engineer at the duPont Plant in Victoria Texas. Mr. Dunglinson had several valuable comments concerning the digraph-fault tree synthesis algorithm and its applicability to chemical processing systems.
1.0 INTRODUCTION

The digraph-fault tree methodology was devised by Dr. Steven Lapp and Professor Gary Powers\(^{(1)(2)}\) for safety analyses of chemical processing systems. The digraph is a multivalued deductive logic diagram that describes the interrelationships among process variables. In addition, events which change or nullify the relationships among process variables are shown. These events appear as basic events in the fault tree. The digraph is in essence an intermediate step between the system schematic and the construction of a fault tree.

For the procedure, one ideally starts with the basic laws of mass, energy and momentum and constructs differential and algebraic equations that describe relationships which exist among system variables, e.g., temperature, mass flow, pressure. The digraph procedure takes a continuum of possible values of variables and uses discrete logic to model the continuum with functional models. These models are useful in failure analysis. For example, complex laws describe heat balances for heat exchangers. A functional model tells us that a decrease of the flow of cooling water to a heat exchanger will cause an increase in the output temperature of the hot stream. These functional relationships are embodied in digraphs.

The digraph procedure was devised for failure analysis of control systems. Manual fault tree techniques in general do not work well in modeling control systems because it is difficult to envision the topology of the system control loop structure from the system schematic when manually constructing a fault tree. This structure may exclude events that can occur in the fault tree at the "local" level—local in the sense of what is immediately necessary and sufficient to cause an event. These logical consistency checks are an important part of the procedure.

The digraph clearly displays the system control loops. Its structure describes how variables are linked at the system level. The synthesis algorithm, which transforms the digraph into a fault tree for a specified top event, requires that the control loop structure in the digraph be found. Finding the loop structure allows two important steps to be conducted in the digraph-fault tree procedure.
• By knowing the dynamics of the relationships between the variables, one can assess the dynamics of the response of the control loops.

• One can locate trigger nodes on the control loops. These nodes define the operators to be used. These operators are used as "templates" which transform the digraph into the fault tree.

The digraph-fault tree procedure consists of two basic steps which are particularly efficient in the analysis of complex systems.

Step I—Identification of (1) the cause and effect type of relationships between variables (edges) and (2) "unusual" system states (component failures, basic event states, etc.). This information is displayed in the system digraph.

Step II—Construction of the fault tree. The Lapp-Powers' operators which transform the digraph into the fault tree.

Conventional fault tree synthesis requires the analyst to consider all aspects simultaneously.

The digraph-fault tree procedure also gives a systematic format for the analyst to consider the failure modes and unusual states for all components and variables.

Another useful feature of the digraph-fault tree procedure is that multivalued logic can be considered. Variables are "discretized" into five possible values, namely: normal, moderate (high or low), and large (high or low.) Values of variables other than normal values are called disturbances similar to "perturbation variables" in control theory. Control loops are classified according to their ability to cancel a disturbance of a given size or vice versa. Control loops may fail to cancel disturbances because control devices are inactive (eg. control devices fail in the "stuck" mode) or the control loops may be the cause of the disturbance if control devices fail high or low. Hence, classifying failure modes of control devices is also an important part of the procedure.
The digraph-fault tree methodology has been successfully applied to safety analyses of chemical processing systems\(^2\) and to security system analyses.\(^3\) The next section of this paper describes this methodology and cites examples of its use in modeling chemical processing and security systems. This description will facilitate an understanding of its application in modeling transportation systems, which is the third section of this paper. Emphasis is given to the importance of modeling a human operator as the control element in a transportation system. For the case in which transportation systems have automatic control, e.g., the Bay Area Rapid Transit train control system, the discussion of chemical process control is directly applicable.

The fourth section discusses the application of this method to the marine mode of transportation. An example is taken from a study performed for Cabot Corporation which analyzed the effectiveness of special coast guard rules in preventing a collision between a liquefied natural gas (LNG) tanker and a potential striking vessel in Boston Harbor. This study is described by Barlow and Lambert\(^4\) who used standard fault tree techniques in generating collision scenarios involving an LNG tanker. It is shown how additional insight and information, such as dynamics and human factors, can be gained by applying digraph-fault tree procedures, and how this can lead to better estimates of accident probabilities for transportation systems.
2.0 DIGRAPH-FAULT TREE METHODOLOGY

The purpose of the digraph-fault tree methodology is to systematically produce a fault tree for qualitative and quantitative evaluation. A fault tree is a deductive Boolean logic model of a Top Event, an undesired event or system state. Top Events are events such as "fire," "explosion," or "system shutdown" for safety and reliability analyses. For modeling hazardous materials transportation, the Top Event is the occurrence of the initiating event in the accident sequence. The initiating event is defined as the initial deviation from normal activities of the transportation system. Train derailments and ship or highway collisions (circumstances necessary for breach of containment of the hazardous material) are examples of initiating events and Top Events to fault trees for transportation systems. The Top Event is defined in terms of basic events which provide the limit of resolution for the fault tree.

The basic events in safety and reliability analyses include human error, equipment failure, and environmental conditions. Fault trees for transportation accidents contain these events with additional emphasis placed on modeling failure of human response in preventing the accident.

Historically, fault trees have been constructed manually by using established rules. These rules define the logic gates to be used and the input to these gates. A number of disadvantages exist in traditional fault tree analysis (FTA). For example:

- Rules for manual fault tree construction do not provide for consistency checks and give no explicit basis for the generation of AND gates.
- Analysts can infer differing cause-and-effect relationships when analyzing a system schematic, causing the construction of different fault trees for the same problem.
- Dynamics and multivalued logic are difficult to incorporate in FTA.
To partially alleviate these disadvantages, directed graphs, called digraphs, are used to construct fault trees. Some of the advantages over traditional FTA are the following:

- Unit model digraphs are constructed for individual components. The cause-and-effect relationships are clearly displayed in these unit models as well as the level of detail in the modeling.
- The system topology with regards to information flow and control loops are displayed in the system digraph.
- Multivalued logic and the direction and deviations in the system variables are incorporated, as well as component failures.
- The dynamics of the relationships of system variables can be considered.
- A transformation algorithm is devised which generates a fault tree from the system digraph. The algorithm states explicitly when to use AND gates and OR gates, and uses consistency checks in constructing the fault tree.
- The digraph-fault tree procedure is a two-step process. The advantage of using this procedure is that the understanding of the relationships between process variables is established and formalized before fault tree synthesis begins.
- The procedure is a "structured" approach which helps to ensure that "all" failure modes are considered.

2.1 FAULT TREE SYNTHESIS AND EVALUATION SCHEME

Figure 1 describes how Lapp and Powers use digraphs in generating fault trees of chemical processing systems. They start with a process flow diagram that describes (1) input-output process flow streams, (2) connectivity of equipment, and (3) means for process control. On the basis of property data, an assessment of hazards is made. The Top Events to fault trees, which correspond to disturbances in process variables (e.g., loss of cooling water to a chemical reactor), are identified. The system digraph is generated from equipment safety models called unit model digraphs, the basic building block of the procedure. The limit of resolution is primal variables and equipment failure. Primal variables represent variables such as electricity, air and other utility services. Losses of these services are basic events in the analysis.
FIGURE 1
THE LAPP-POWERS' FAULT TREE SYNTHESIS AND EVALUATION SCHEME
The fault tree is synthesized via a transformation algorithm that describes the combination of basic events involving equipment failure and disturbances in primal variables that cause the Top Event. The algorithm requires that the system control loops in the digraph be found and that the dynamics of the control response be assessed. Basically, the algorithm delineates how control loops fail in either causing or passing disturbances which cause the Top Event. Lapp and Powers evaluate the fault tree both qualitatively and quantitatively to find the system failure modes (called the min cut sets) and occurrence frequencies of the Top Event. Recommendations concerning the safety of the system are based upon these evaluations. The fault tree can be modified to determine the quantitative effect of alternate "corrective" measures.

2.2 TERMINOLOGY AND NOTATION

The reader is referred to Appendix A for the glossary of terms used in the Lapp-Powers fault tree synthesis algorithm.

A digraph is a set of nodes and connecting edges. Nodes in the digraph represent variables. If one variable affects another variable, a directed arrow or edge connects the independent variable to the dependent variable. The directed edge may either be a normal edge which indicates that the relationship is normally true, or a conditional edge which indicates that the relationship is true only when another event (or condition) exists. Edges connecting a given pair of nodes are mutually exclusive; only one edge relationship is true at a given time.

Numbers may be placed on the directed edge to represent the gains (i.e., relationships) between the two variables. These gains are based on the mathematical definition of gain, \( \frac{\partial Y}{\partial X} \), where \( X \) and \( Y \) denote the independent and dependent variables, respectively. Gains of 1 represent moderate relationships between variables, gains of 0 indicate the nullification of any relationship existing between the two events, and gains of 10 indicate strong relationships between variables.

Variables in the digraph are represented by alphanumeric labels on the nodes. For instance "P2", "M3", "FIRE at HX" represent pressure at location 2, mass flow rate at location 3, and fire at heat exchanger, respectively. The direction
of the deviations from "normal" in the variables are denoted by "+" and "-". A deviation of a magnitude of 1 indicates a range of values that is considered moderate. A magnitude of 0 represents a true or expected range of values of the event. A magnitude of 10 indicates a large disturbance. The classification "large" versus "moderate" (i.e. ± versus ± 1) is usually based on the ability of the system to control the deviation—a ± 10 implies a change beyond the capacity of the system to compensate. The same scheme of -10, -1, 0, +1, +10 is also used to represent the deviations in the values of events. For instance P2(0) represents the true or expected value of pressure at location 2, and M3(+1) represents a moderate mass flow rate at location 3. M3(-10) represents a large drop in mass flow rate at location 3. In general, moderate disturbances (+1 or -1) are expected to occur. Negative feedback loops can cancel these disturbances. Large disturbances occur rarely and in general cannot be canceled by negative feedback loops. Large can be due to magnitude and/or dynamics. Some variables may be univariant; that is, they deviate only in the positive direction or only in the negative direction. For instance, "FIRE at HX" is a univariant variable - i.e., it either occurs (+1) or it does not occur (0).

Figure 2 serves as an example that will aid in understanding the terminology and notation of the digraph-fault tree procedure. A pneumatic air-to-close regulating control valve is shown. Regulating the controller air pressure at location 3 (represented by variable P3) will adjust the position of the valve, which will in turn regulate the flow cross-sectional area of the control valve and thus control the mass flow rate at location 2 (i.e., variable M2). Since the valve is air-to-close, increasing (decreasing) P3 will decrease (increase) M2, resulting in a -1 gain between P3 and M2. A gain of -1 implies that M2, the independent variable, and P3, the dependent variable, will have the relationship given in Figure 3.

If the control valve in Figure 3 were quick closing (ON-OFF), increasing P3 slightly quickly shuts the valve and causes mass flow rate to instantaneously go to zero (i.e., M2 = -10). The mapping for this relationship is shown in Figure 4.

Losing air pressure does not open the valve any further which explains the first two rows corresponding to zero value of M2, the "normal" value.
FIGURE 2
GAINS BETWEEN PROCESS VARIABLES
FIGURE 3
MAPPING FOR REGULATING CONTROL VALVE WITH GAIN -1

FIGURE 4
MAPPING FOR QUICK CLOSING CONTROL VALVE, GAIN -10
Note a +10 disturbance in the independent variable with a -10 gain causes a -10 disturbance in the dependent variable. The absolute the maximum value a dependent variable can assume is 10 (not 100).

The general rule for determining the value of the dependent variable is to multiply the value of the independent variable times the gain, noting that the absolute value of output variable cannot exceed 10.

Other events may change or reverse the relationship. In the case of the regulating control valve, reversing the valve action would cause the valve to be air-to-open, changing the gain to +1. If the valve were stuck in its normal position, changing controller air pressure has no effect on M2, i.e., there is a zero gain between P3 and M2.

2.3 EDGE-DEPENDENT RELATIONSHIPS

Other gain relationships, called edge-dependent relationships, depend upon the value of another variable (which represents an event). As an example, consider Figure 5 which represents a system in which there is mass flow between locations 3 and 4, resulting in a +1 gain between T3 and T4 where T denotes temperature. If mass flow stopped at location 3, i.e., $M3 = -10$ (the edge relationship), then there exists no relationship between T3 and T4, resulting in the zero gain relationship.

It is important to note that the value of the gain is entirely different from the value of the variable. Values of gains appear on the digraph – never in the fault tree. Values of variables, which are events, appear in the fault tree. The only case where events appear in the digraph are the conditional edge relationships.

2.4 UNIT MODEL DIGRAPHS

Figure 2 embodies the relationships for a unit model digraph of a pneumatic air-to-close control valve. The information to construct these unit models are obtained from the basic laws of energy, mass and momentum and from failures modes and effects analysis. The unit model digraph can be thought of as a transfer function for devices. Unit model digraphs are similar in scope to mini fault trees described by Fussell(5) and decision tables described by Salem, et al.(6)

2-8
Edge

Conditional edge

FIGURE 5
EDGE RELATIONSHIPS
2.5 CONTROL LOOPS

As mentioned in the introduction, an important part of the digraph-fault tree procedure is to be able to model a system as a control system. There are two basic control types of loops:

- Negative feedback loops
- Negative feedforward loops

The basic elements to control loops are:

- The Sensor
  Senses a variable (called the sensed variable) and sends a signal to the controller

- The Controller
  Compares the actual value of the sensed variable to the desired value and derives a corrective signal from any deviation

- The Control Device
  Is commanded by the controller to manipulate a variable called the manipulated variable to counteract disturbances in the sensed variable

The controller in chemical process control is a physical device which senses disturbances in sensed variables by comparing the actual value of the variable (output from the sensor) with the desired value which determines the set point on the controller. The control loop is calibrated by adjusting the set point on the controller. Any difference between the actual value and desired value is compensated for by changing the value of a manipulated variable (changing the pressure on the bonnet of a control valve that regulates flow of cooling water to a heat exchanger is an example of this).

The same methodology can be used in trying to model human response in preventing the occurrence of transportation accidents. A human operator is both
the sensor and controller. In transportation systems he senses variables such as approach distance, incident angle, hazards in terrain, and makes an assessment of the desired values of these variables. Any undesired values are compensated for by changes in speed or direction. In short, modeling of humans in transportation systems can be described as follows. A human senses input stimuli, makes decisions regarding the abnormal occurrence of these stimuli, and takes corrective action to prevent an accident.

We now describe basic feedback and feedforwards loops in terms of the digraph-fault tree procedure. The examples we choose are for chemical processing systems. It is shown later that digraphs for transportation systems can be constructed and analyzed in a similar manner.

2.6 FEEDBACK LOOPS

Negative feedback loops (NFBL's) correct moderate or large disturbances in process variables. A NFBL senses a disturbance in a variable (called the sensed variable) and commands the manipulated variable to deviate in such a manner as to counteract the effect of the given disturbance.

An example of a digraph for a NFBL is shown in Figure 6. A NFBL in a digraph is a path which starts and ends at the same node and the product of the normal gains around the loops is negative.

In Figure 6, the nodes Fire and T2 represent external disturbances to the NFBL entering at node T3.

Positive feedback loops enhance deviations in process variables. In this case input and output variables have the same sign.

We give two examples to illustrate feedback loops. For these examples, all controllers are reverse acting, i.e., they invert the signals they receive—an increase in the input signal causes a decrease in the output signal. On the other hand, sensors have a positive gain, i.e., an increase in the input signal to a sensor causes an increase in the output signal.
- Path in digraph which starts and ends at same node
- Product of normal gains around loop is negative

FIGURE 6
NEGATIVE FEEDBACK LOOP (NFBL)
Figure 7, taken from Reference 2, shows a flow control NFBL. The system senses flow at location 2 and adjusts the valve to maintain flow at the set point value. To construct the digraph, we start at location 2, and ask what could cause changes in $M_2$, i.e., what is (are) the local input variables. The answer to this question is $P_5$, the controller air pressure. Hence $P_5$ is connected to $M_2$ with a $+I$ gain. We proceed backwards (i.e., deductively) and ask what can cause changes in $P_5$? The answer is $P_4$ with a $-I$ gain since the controller is reverse acting. $P_4$ is the sensor output, $M_2$ is the sensor input. At this point, the loop is completed. The loop is a NFBL since the product of the normal gains is $-1$. This implies, for example, that a positive disturbance in $M_2$ would result in a corrective action in causing $P_5$ to go negative and eventually cause $M_2$ to return to its normal value (the "0" value).

Another example is shown in Figure 8 of a feedback loop. In this system, nitric acid, $HNO_3$, is mixed with water. The flow of nitric acid is controlled by sensing the pH at location 4. We proceed in a similar manner as described above, starting at node $M_2$. The gain between $M_2$ and $pH_4$ is $-I$ since pH represents the negative of the common logarithm of the hydronium ion, $H^+$, concentration. Increasing $M_2$ corresponds to increasing the $H^+$ concentration.

The feedback loop shown in Figure 8 is a positive feedback loop. In actual practice a PFBL would only occur as a result of human error either during startup or during maintenance. Instead of correcting a disturbance, a PFBL will worsen the disturbance. In this case, the loop will amplify noise. Noise is any randomly occurring perturbation in a system variable that is expected to occur. The control valve shown in Figure 8 will open and shut in a periodic fashion. A reversal of a control device or an improperly designed control loop would cause the loop to be positive. Normally, this system fault is detected during startup or just after maintenance when the controller is placed in the manual mode. In the manual mode, the controller is inactive and the operator takes the place of the controller by regulating the position of the valve.

2.7 FEEDFORWARD LOOPS

A disadvantage of feedback control is that the disturbance in the sensed variable exists for some finite time before the loop can cancel the effect of the disturbance.
FIGURE 7
FLOW CONTROL NEGATIVE FEEDBACK LOOP
FIGURE 8
pH CONTROL POSITIVE FEEDBACK LOOP
Feedforward control, if working perfectly, can exactly cancel a disturbance in a variable by sensing an upstream variable and manipulating a downstream variable. In practice, a disturbance cannot be cancelled exactly in feedforward control. Generally in the chemical processing industry, feedforward control is combined with feedback control.

Two examples of feedforward control in the chemical processing industry are:

- Changing set points on controllers for varying grades of crude oil (in the refinery industry)
- Shutting down a system in the event of the loss of a critical component such as a cooling water pump

Most corrective actions taken by humans in transportation systems are feedforward control.

Figure 9 shows a generic negative feedforward control loop, NFFL. The NFFL is two or more paths from one node to another node in the digraph. The sign of the product of the normal gains on one of the paths is different from the others. The path with the net positive gain on which disturbances propagate is called the causative branch. The path with the net negative gain which provides the cancellation action is called the corrective branch.

Figure 10 shows an example of negative feedforward control. Temperature of the input stream at location 1 is sensed and any deviation in this temperature is corrected by manipulating the flow of cooling water at location 1. This in turn maintains the output temperature, T3, at its desired value.

If the temperature sensor in Figure 10 were located on the output stream, stream 3, then the control loop would be a NFBL. In this case, the loop is capable of correcting any moderate deviations of the following variables: T1, M1, T7 and M7 where T denotes temperature and M, mass flow. However, it must be noted that the NFFL in Figure 10 is capable only of correcting disturbances in T1.
- Two or more paths from one node to another different node in digraph

- Sign of the product of normal gains on one of the paths is different from others

FIGURE 9
NEGATIVE FEEDFORWARD LOOP (NFFL)
CAUSATIVE BRANCH

CORRECTIVE BRANCH

FIGURE 10
NEGATIVE FEEDFORWARD TEMPERATURE CONTROL
Figure 11 shows a mixing tee that is positive feedforward control. Both branches have a positive gain.

2.8 SYSTEM DIGRAPH CONSTRUCTION

Construction of a digraph was discussed briefly in Section 2.6. The system digraph is constructed in a similar manner as a fault tree. One starts with a Top Event variable and through examination of the system schematic, which displays energy and information flow, determines the local input variables. When at all possible, unit model digraphs are used to link the system digraph.

Variables which have inputs are developed further. If control loops exist in the system, then it is possible to trace through the same variable twice. Variables which have already been developed should not be retraced. Variables which are conditions are developed in the same manner as input variables. The process is terminated when all variables have no inputs, i.e., primal variables are encountered.

2.9 SYNTHESIS ALGORITHM

We now discuss the most difficult part of the digraph-fault tree procedure, the synthesis algorithm which constructs a fault tree from the system digraph. In order to facilitate understanding of the algorithm, we discuss simple algorithms for three types of digraphs:

- Digraphs with no control loops
- Digraphs with one NFBL
- Digraphs with one NFFL

We then consider a very important part of the procedure, the classification of control loops according to their range and dynamics. Lastly, we discuss the general synthesis algorithm for digraphs with multiple control loops which can be described in terms of the simple algorithms listed above with consideration given to dynamics.
FIGURE II
MIXING TEE POSITIVE FEEDFORWARD LOOP
We will now discuss construction of fault trees from digraphs with no control loops.

Figure 12 represents a shell-and-tube heat exchanger. The hot stream enters at location 1 and exits at location 2. The cooling stream enters at location 3 and exists at location 4. The digraph for Top Event Node T2 is also shown in Figure 12. The Top Event we wish to construct a fault tree for is T2(+I), i.e., T2 moderately high. Since there are no control loops in the system, any one of the input disturbances can cause T2(+I). The resulting fault tree is shown in Figure 13 which consists of OR logic.

We do not allow randomly occurring disturbances to fortuitously cancel each other. For example, if the temperature of the input stream 1 increase (i.e., we have T1(+I)), and simultaneously the mass flow of cooling water increases (i.e., we have M1(+I)), then the output temperature would remain at its normal value (i.e., T2(0)). However, we do not allow this. We are in essence following D. Haasl's rule of fault tree construction:

Expect no miracles; those things that normally occur as the result of a fault will occur, and only those things. Also, normal system operation may be expected to occur when faults occur.

Stated in other terms, when disturbances in variables or equipment failure occur, we do not take credit for other failures that may rectify the effect of the given disturbance or failure. This rule is an accurate and conservative approximation for reliable systems in which system failure is rare.

We may make the general statement that if a system digraph contains no control loops or conditional edge statements, then the fault tree consists of all OR gates with basic events representing either (1) disturbances in primal variables, (2) equipment failure, (3) human error, or (4) environmental conditions.

Next, the topic of constructing fault trees for digraphs with simple NFBL's is discussed.
FIGURE 12
DIGRAPH FOR HEAT EXCHANGER
FIGURE 13

FAULT TREE FOR HEAT EXCHANGER
As we work backwards on the digraph providing inputs to the fault tree and encounter a variable on a NFBL, then a special operator must be used in constructing the fault tree. Checks for logical consistency become important since, as discussed below, the Top Event for a NFBL changes depending on where one encounters the first variable on a NFBL working backwards from the Top Event variable. This first variable is called the original point entry on the NFBL.

Three types of failure for control devices on NFBL's must be considered in the operator:

- Inactivation of control devices causing zero gains on the NFBL, e.g., controller-broken or sensor-broken
- Reversal of control devices causing a reversal of gains on the NFBL, e.g., reversed-valve-action or controller-action-reversed
- Control devices failing high or low causing a disturbance on the NFBL

In addition, two types of external disturbances entering the NFBL must be considered:

- Moderate disturbances
- Large or fast disturbances

The negative feedback loop operator is described in terms of an example given in Figure 7. The operator described in this report considers the loop in its entirety when constructing the fault tree. Lapp-Powers use their NFBL operator recursively node-by-node around the loop. Both operators yield basically the same results for simple NFBLs. However, the authors have found that the operator is easier to explain when the loop is considered in its entirety.

Before discussing the operator, the system in Figure 7 is described. The process is a simple feedback loop for flow control. The flowrate of stream 3 (M3) is sensed by a flow sensor connected to signal line 4. As the flow increases, the
signal in line 4 increases. The flow recorder-controller upon receiving the increased signal from 4 sends a decreased signal to stream 5. This causes the valve to close returning the flow to its desired setting.

Discussions with the designer and process operator indicate that the following events are known to occur in this process:

Sensor: Fails (High, Low, Stuck), reversed

Controller: Fails (High, Low, Stuck), on manual, loss of air (causes signal 5 to go down), reversed

Valve: Fails (Open, Closed, Stuck, Stuck and Releases), reversed

The system is normally digraph mapping operating with flow in lines 1, 2, and 3. The control system can rectify the effect of a partial loss of controller air but not a total loss. We wish to discuss the operator which will generate the "correct" fault tree for the event, M3(+1).

The system digraph is displayed in Figure 14. The NFBL consists of nodes M2, P5 and P4. The nodes between M2 and P5 represent the unit model diagraph for the valve, between P5 and P4, the flow controller and between P4 and M2, the flow sensor. The nodes which represent control devices failing high or low are represented by univariant variables (with values 0 or +1 i.e., either they occur or not). Since the gain associated with these nodes is 10, they represent large external disturbances. This is because all input nodes to the NFBL in Figure 14 represent exclusively large disturbances except for two nodes, M1 and controller air. These nodes represent either moderate or large disturbances. Working backwards from M3, node M2 is encountered which is on a NFBL.

The three ways that a NFBL either causes or passes a disturbance is given below:

- A gain reversal of a control device transforms the loop to a PFBL.
- An external disturbance too large or fast for the control loop to correct enters the loop.
FIGURE 14
DIGRAPH NEGATIVE FEEDBACK FLOW CONTROL SYSTEM
• A moderate external disturbance enters the loop and the loop is inactive because one or more control devices are inactive.

The NFBL operator is displayed in fault tree form in Figure 15. The left-hand input describes the situation in which the loop is positive because an odd number of control devices are reversed. (This situation was discussed in Section 2.7.) In this case, the NFBL is the cause of the disturbance. Since one reversal is sufficient, we do not consider three, five etc., reversals since these events yield non-minimal cut sets. Also, we do not allow for the fortunate circumstance of allowing an even number of control devices to be reversed causing the loop to be negative again. If we do, we are violating D. Haasl's rule since we are allowing a failure to rectify the situation.

Since reversal events are single-event minimal cut sets, we do not consider them again in the operator.

The next fault tree inputs to be considered are large or fast disturbances, that is, too large or fast for the loop to correct. These disturbances are sufficient to fail the NFBL. Not all nodes represented in Figure 14 cause $M_3(+)$. Some cause $M_3(-)$ and we must select only those large input disturbances that can cause $M_3(+)$.:

- $M_1(+)$
- Valve fails mechanically open**
- Controller Set Point High**
- Controller fails High**
- Large increase in Controller Air (+10)
- Flow sensor fails low**
- Line 4 rupture

The events with double asterisks represent control devices failing high or low. When this happens, the loop characteristics change so that the loop corrects high
Deviation of variable on negative feedback loop

OR

Noise drives positive loop unstable

AND

Noise (true) Loop is positive (odd number of devices reversed)

OR

Large or fast external disturbances enter the loop cause deviation of variable on negative feedback loop

Moderate external disturbances enter loop cause deviation in loop variable

n possible inputs

Moderate external disturbances enter the loop at node j cause deviation in loop variable

AND

Moderate external disturbances enter at node j

Upstream control devices from node j to node 1 inactivated

*n = number of nodes on the system digraph for the negative feedback loop

Node 1 is the original point of entry on the negative feedback loop

FIGURE 15
NEGATIVE FEEDBACK LOOP OPERATOR
or low. For example, suppose that loop were designed to maintain the output flow at five gallons per minute. If the set point was set high, the loop would adjust to a higher normal value, say eight gallons per minute.

The third input in Figure 15 represents moderate external disturbances entering the NFBL and causing M2(+1).

The operator gives special attention to the location where moderate disturbances enter the NFBL (see Figures 15 and 16). Moderate disturbances are by definition those which the NFBL is able to cancel. For a moderate disturbance entering a NFBL to cause a deviation of a variable on the NFBL, the following conditions must be met (refer to Figure 16).

- No control devices are inactivated from the point the disturbance enters the loop downstream to the loop variable under development (the term downstream means in the same direction as the arrows are pointing in the digraph).
- At least one control device is inactivated on the remainder of the loop. Inactivated means in the "stuck" mode so that another disturbance is necessary to fail the NFBL.

Condition 1 permits the disturbance to propagate down the loop. It implies that the inactivation edge changes as one proceeds backwards from the original point of entry on the NFBL.* Condition 2 inactivates the loop so that no corrective action from the NFBL is possible.

Erroneous min cut sets can be generated if the cut sets include downstream inactivated control devices. For example, the controller air pressure going high would have no effect on a control valve that is stuck. Hence, M2 would remain at its normal value and not deviate to the +1 state.

---

* This implies a different fault tree may be generated depending upon the original point of entry on the NFBL. As pointed out in the introduction, this is why, in some cases, an analyst cannot generate "local" equations and generate a correct fault tree.
Variable under development in Fig. 1. original point of entry on negative feedback loop

Disturbance

One or more control devices inactivated

FIGURE 16

FAILURE OF NFBL FOR EXTERNAL MODERATE DISTURBANCES
The resulting fault tree for $M_3(+1)$ is shown in Figure 17. Note the multivalued logic, i.e., $M1(+10)$ and Controller Air Pressure ($+10$) appears as well as $M1(+1)$ and Controller Air Pressure ($+1$).

The last operator to be discussed is the negative feedforward operator. This operator will be used extensively in generating fault trees for transportation systems. Recall from the discussion in Section 2.7, that an NFFL cancels disturbances only when they enter at the node which starts the NFFL. If a disturbance enters anywhere else on the loop, the disturbance will propagate through the loop.

In order to invoke the NFFL operator, a disturbance in the node which terminates the NFFL must appear in the fault tree. Within the domain of that event, appears an event that represents a disturbance in the node which starts the NFFL. (We are working backwards on the diagraph from end to start, constructing the fault tree.) At this point, the NFFL has failed to cancel the disturbance. This means that the disturbance entered the NFFL, propagated down the causative branch and that the corrective branch failed to cancel the disturbance. The AND gate is in essence the NFFL operator and is invoked on the node on the causative branch just before the start of the NFFL working backwards. The corrective branch fails to cancel a disturbance if either one of two conditions occur:

- A control device on the corrective branch is inactive (zero gain events), causing the NFFL to be inactive
- A control device on the corrective branch is reversed causing the loop to be positive

Note that a reversal of a device is not sufficient to cause a disturbance since a positive feedforward loop does not amplify noise like a positive feedback loop does.

As an example of the use of the NFFL operator, consider the system shown in Figure 10. The process shown tries to maintain $T_3$ at a set temperature by
FIGURE 17

FAULT TREE FOR M3(+1) NFBL FLOW CONTROL
Noise drives positive loop unstable and causes M2(+1)

\[ \text{AND} \]

System noise (true)

\[ \text{OR} \]

Loop is positive

Valve reversed

FRC reversed

Flow sensor reversed
Large external disturbances enter the loop and cause M2(+1)

OR

M1 (+10)  Valve fails mech  open
         Set pt high
         FRC fails high
         Flow sensor fails low
         Line 4 rupture

FIGURE 17
(CONT.)
Moderate external disturbances enter inactive loop and cause M2(+1)

AND

Moderate external disturbance enters loop

M1(+1)

Loop is inactive

OR

Valve stuck

FRC stuck

FRC on manual

Flow sensor stuck

FIGURE 17
(CONT.)

2-35
MODERATE EXTERNAL DISTURBANCES ENTER INACTIVE LOOP AT P5 AND CAUSE M2(+1)

MODERATE EXTERNAL DISTURBANCE ENTERS LOOP AT P5

CONTROLLER AIR PRESSURE (+1)

UPSTREAM CONTROL DEVICES ARE INACTIVE

OR

FRC STUCK

FRC ON MANUAL

FLOW SENSOR STUCK

FIGURE 17
(CONT.)
sensing the temperature of Stream 1 and changing the flow of cold fluid in Stream 7. A digraph for Top Event Node T3 is shown in Figure 18. The node T1 starts the NFFL, node T3 terminates the NFFL.

The fault tree is shown in Figure 19. The distinguishing features of this fault tree are listed below:

- Disturbances in variable T1 is primal (i.e., a deviation in T1 is considered a basic event.
- An AND gate is generated when input disturbances cause T2(+1) from node T1. T2 is the node on the causative branch just before the start of the NFFL.
- NFFL will not handle large disturbances in T2, i.e., T2(+10). The control valve in this case is in the full open mode and cannot open any further.
- Local reversals in conjunction with other events are considered (e.g., see inputs to event M7(-1)).
- If T2 were the Top Event Node, the AND gate would not be generated since disturbances in T3 do not appear in the fault tree.
- If T2 had other input nodes other than T1, then disturbances from these nodes would not generate an AND gate since these nodes do not activate the NFFL.

The NFFL loop operator is shown in Figure 20. It embodies all the considerations listed above for the fault tree in Figure 19.

The operator presented in Figure 20 was used many times in a Lawrence Livermore Laboratory study that generated fault trees for assessment of security systems, called material control systems. The purpose of a material control (MC) system is to prevent theft of Special Nuclear Material (SNM), such as plutonium, from nuclear facilities. The MC system consists of procedures, monitors, computers and a security force designed to prevent theft, both covertly or overtly. The Livermore study focused on the covert threat, i.e., the insider problem. A prototype facility called the Test Bed was designed. The assessment of this facility generated a system diagraph with Top Event Node
FIGURE 18
DIGRAPH NEGATIVE FEEDFORWARD TEMPERATURE CONTROL SYSTEM

Ext. fire at heat exchanger
1 (temp sensor stuck)
0 (temp sensor stuck)
+1 (TRC reversed)
-1 (TRC on manual)

Temp set point
FIGURE 19
NEGATIVE FEEDFORWARD TEMPERATURE CONTROL SYSTEM
FAULT TREE
Corrective branch is inactive due to zero gain events

Corrective branch of positive feedforward loop fails

Temp sensor stuck

TRC on manual

Control valve stuck

Temp sensor reversed

TRC reversed

Control valve reversed

FIGURE 19
(CONT.)
FIGURE 20
NEGATIVE FEEDFORWARD LOOP OPERATOR
Successful theft of special nuclear material from Test Bed

Adversary movement out of Test Bed from removal node

Guard and personnel location monitors

Special nuclear material flow to removal node from source

Process monitors and controls

Process or procedure anomaly states

Safeguards system response

Computer decision logic

Initial conditions
- Removal node
- Adversary at removal node
- Container at removal node

FIGURE 21
GENERAL FORM OF SYSTEM DIGRAPH FOR TEST BED
"Successful theft of SNM from the Test Bed" (see Figure 21). As the adversary commits acts necessary to steal SNM, a series of NFFL's are activated called cancellation loops which generate a safeguards response in preventing the adversary from stealing SNM. For the adversary to be successful, all these loops must fail. These loops fail as a result of:

- Random monitor failure
- Inadequate monitor measurement sensitivity
- Human error, including slow guard response
- Adversary activity, including equipment tampering and collusion

The synthesis algorithm creates an AND logic gate in the fault tree each time a cancellation loop in the system digraph fails.

Once generated, the fault tree was evaluated qualitatively and quantitatively to assess the vulnerabilities of the safeguard system. An assessment of the dynamics of the safeguards response was also made. The min cut sets to the fault tree are called the adversary event sets.

As described in Sections 3, 4 and 5, the NFFL operator will be a key operator in the risk analysis of transportation systems.

Thus far, we have presented simple operators for negative feedback and feedforward loops. Before discussing the general algorithm, we must discuss dynamics and ranges for control loops.

In process control, two parameters determine the dynamic response of control loops to disturbances (i.e., dynamics associated with gains):

- Dead time,
- Time constant(s),
As an example of dead time, consider fluid flowing in a section of pipe of length \( L \) with linear velocity \( V \). A change of temperature would take \( L/V \) time units for the temperature to change \( L \) units of distance away.

For a first order response, the time response to a step change \( \Delta X \) in the independent variable is:

\[
Y(t) = Y_0 + \Delta Y(1 - \exp(-t/\theta))
\]

Where

\[
\begin{align*}
\Delta Y &= Y_\infty - Y_0 \\
\theta &= \text{First order time constant} \\
Y_0 &= \text{Value of the dependent variable at } t=0. \\
Y_\infty &= \text{Value of the dependent variable at } t = \infty
\end{align*}
\]

If dead time exists in the system, the above expression becomes:

\[
Y(t) = Y_0 + \Delta Y(1 - \exp(-t-\tau)/\theta)
\]

for \( t \geq \tau \).

This relationship is plotted in Figure 22.

In considering human response, there is also a dead time and reaction time as there is in chemical processes. We consider these factors in the system described below.

Also, in this system, we discuss how to classify control loops according to range. These concepts are important in modeling transportation systems.

The system given in Figure 23, discharges gas from a reservoir into a pressure tank. The pumping cycle is initiated by an operator who manually resets a timer which causes the timer contacts to close and the pump to start. The switch is
FIGURE 22
DYNAMICS ASSOCIATED WITH GAINS

\[ Y_0 + \Delta Y \]

\[ Y_0 \]

\( \tau \)

TIME
FIGURE 23
PRESSURE TANK SYSTEM
normally closed. At a prescribed time later (well before any overpressure condition can exist), the timer times out and the timer contacts open. Current is denied to the pump and pumping ceases. If the timer contacts do not open, the operator will notice the tank pressure by the pressure gauge becoming too high and he will open the switch. Again current is denied to the pump and pumping should cease. It is assumed after each cycle, the compressed gas is discharged by opening the valve. It is also assumed that the valve is closed before the next cycle. Let $T_r$ correspond to the time necessary for tank rupture to occur after the timer contacts are supposed to open. Denote the reaction time of the operator responding to a high pressure reading and opening the switch as $T_o$.

The digraph with tank pressure as the Top Event Variable, is shown in Figure 24. The subsequent fault tree which uses the synthesis algorithm is shown in Figure 25. There are two negative feedback loops consisting of the following devices:

- The pressure relief valve
- The switch, operator and pressure gauge

The failure modes for these devices appear as zero gain events in Figure 24. Both of these loops must fail to cause overpressure.

The range of the NFBL for the pressure relief valve is a $+10$ disturbance. The timer contacts failing to open is an external disturbance to the operator-controlled negative feedback loop. It is a disturbance that integrates over time causing the tank pressure to increase in time. In order to perform a dynamic assessment of the loop, an experiment must be conducted to determine the fraction of the time that the operator is successful in preventing an overpressure condition. If the pump were very large and the tank very small, the operator would have no time to respond and he would never be successful. In this case, the timer contacts failing to open would be a large disturbance (i.e., $+10$) and it is not necessary to consider the failure modes of the control devices on the operator-controlled NFBL since it fails all the time, i.e., the gate event "NFBL inactive"
FIGURE 24
DIGRAPh FOR PRESSURE TANK RUPTURE
PRESSURE TANK RUPTURE

OR

TANK RUPTURES UNDER (NORMAL) LOAD

1

TANK RUPTURE DUE TO OVERPRESSURE AND

PUMP MOTOR OPERATES TOO LONG

AND

RELIEF VALVE FAILS TO OPEN

6

TIMER CONTACTS FAIL TO OPEN

2

DISTURBANCE

NEGATIVE FEEDBACK LOOP INACTIVE

OR

PRESSURE GAUGE STUCK

3

OPERATOR FAILS TO OPEN SWITCH

4

SWITCH FAILS TO OPEN

5

FIGURE 25

FAULT TREE FOR PRESSURE TANK RUPTURE
is always true. For this case, \( T_r < < T_o \). On the other hand, if we have a very small pump and a very large tank, then the operator would have a long time to respond. He would be successful a very large fraction of the time the contacts failed, given that each device on the NFBL worked as intended. In this case, the disturbance is a moderate external disturbance, in which the NFBL is capable of correcting. For this case, \( T_o >> T_r \). In many cases, the response time characteristics of control loops fall between the two extremes stated above. We can add a zero gain event "control loop too slow" (or event too fast) which can appear both in the digraph and fault tree. A dynamic simulation of system behavior can be conducted to determine the probability of this event. This approach allows a convenient way of incorporating dynamics in the probabilistic evaluation of fault trees and is a key feature of the approach to transportation risk modeling presented in this report.

We now discuss the general fault tree synthesis algorithm as described in Figure 26. The algorithm holds true for digraphs containing simple NFBL's and NFPL's. More complicated digraph structures containing, for example, edge-dependent activated control loops or nested NFBL loops, require a more sophisticated treatment. As a matter of fact, Lapp and Powers have developed over 30 algorithms to handle various control loop configurations.\(^{(9)}\) An important part of devising algorithms for new configurations is to envision the control loop structure on the system level, determine how disturbances can propagate through the control loop structure, and determine what restrictions are placed on the local level when constructing the fault tree from the digraph. These considerations were incorporated in the algorithm for the NFBL.

The algorithm presented in Figure 26 (or simple extensions of it) can handle a large number of systems.

We now describe the basic algorithm in Figure 26. The purpose of the synthesis algorithm is to construct a fault tree from the digraph. Starting from the Top Event node, local inputs to this node are found. The algorithms based upon the operators discussed previously construct the fault tree from these inputs. An event is an undeveloped event by definition if its corresponding node on the digraph have inputs, i.e., it is not a primal node, and if these inputs have not yet been incorporated into the fault tree.
1. Select a top event
2. Construct a digraph for the process
3. Find and classify all loops in the digraph (negative feedback (NFBL) and negative feedforward (NFFL) and their range (±1 or ±10)) and perform an assessment of dynamics
4. Are there any undeveloped variables in the fault tree?
   - Yes → Stop
   - No
5. Select one and call it the current output variable

FIGURE 26
LAPP-POWERS' FAULT TREE SYNTHESIS ALGORITHM
6. Is this variable on a NFBL?

- No
- Yes
  - Use NFBL operator
  - Go to step 4

7. Is the variable just before the start of a NFFL and on the causative branch?

- Yes
  - Use NFFL operator
  - Go to step 4
- No
  - Output (value) OR Inputs (value)
  - Go to step 4

FIGURE 26
(CONT.)
The first step in the procedure is to choose a Top Event. A digraph based on the procedure described in Section 2.8 is constructed. All control loops are found in the digraph and an assessment is made concerning their range and dynamics. An example of this assessment was described for the pressure tank system in Figure 24.

Next, the following nodes, called trigger nodes, are located on the system digraph:

- The first node that is encountered on a NFBL working backwards from the Top Event Node (i.e., the original point of entry on the NFBL)
- The node on the causative branch just before the start of the NFFL

These two types of trigger nodes generate, respectively, the NFBL and NFFL fault tree operators described previously. If a node is encountered in the digraph that is not a trigger node, a simple OR gate is generated with disturbances in local nodes as inputs.

Below we summarize the fault tree synthesis algorithm:

1. Top Event corresponds to an undesired change in the Top Event Variable

2. Disturbances on the System Digraph are created in three ways:
   I) Disturbances in primal variables
   II) Equipment failure, human error or environmental conditions
   III) NFBLs cause disturbances as the result of:
       • Loop gain becomes positive (reversal of a control device)
       • Control device fails high or low causing the disturbance
3. NFBLs fail to cancel the disturbance if:
   - They are the cause of the disturbance
   - Large disturbances enter the loop (i.e., the NFBL is too slow or too weak)
   - A moderate disturbance enters the loop and upstream control devices are inactive

4. NFFLs fail to cancel disturbances if:
   - Disturbance enters the NFFL other than at the start of the NFFL
   - Disturbance enters the start of the NFFL and the corrective branch is either inactive or reversed
   - The NFFL is too slow or too weak

5. Conditional edge relationships generate AND gates

6. A disturbance propagates directly through the digraph if there are no control loops.
3.0 TRANSPORTATION RISK MODELING

A concern of the Department of Transportation, DOT, involves the transportation of hazardous materials, such as radioactive waste and chemical substances. DOT is interested in choosing routes which will minimize the risk in transporting these materials. Unfortunately, only nationwide accident event rates exist and are not available for individual routes. One purpose of this report is to present a methodology allowing DOT to choose a route which will minimize the risk.

The approach centers around two steps:

- Devise a methodology capable of generating accident scenarios in terms of basic events in which data exists or can be obtained
- Devise an approach to obtain data for basic events in which data does not exist

Dynamics and the human control elements are important considerations in transportation systems, as well as terrain, traffic frequency and environmental conditions. We feel that the digraph-fault tree methodology can address these considerations as well as generate meaningful scenarios which can be analyzed for assessment of routes.

A transportation system is a control system with accident mitigating features, such as braking, navigation and steering systems.

The differences between modeling a chemical processing system and a transportation system as a controlled system are:

- Definition of the system
- System variables

A chemical processing system is a well defined system with inputs, outputs and means of control clearly delineated. In a transportation system, variables are
always changing--variables such as distance, approach angle and velocity. Depending upon each value of these variables, means of control may be different, e.g., braking or acceleration. These factors must be included when defining a transportation system and in constructing a digraph for the system.

Modeling a transportation system as a control system, while using the digraph-fault tree methodology, requires the following topics to be addressed:

- Define variables in transportation systems
- Model control in transportation systems as feedback and feedforward control
- Incorporation of dynamics

Because system variables change in transportation systems, the "normal" value, i.e., the "0" value, also changes. Hence, it is important to make system variables location specific, and define these variables in terms of each system's environmental conditions, e.g., weather, grade, frequency of traffic, etc. The effectiveness of accident mitigating systems changes with each change in condition. A case in point is a wet railroad track.

The next consideration is the modeling of control loops in transportation systems. Many automatic controls do exist in transportation systems; and these systems can be modeled exactly the same way that chemical control systems were in the previous section. Many control loops exist precisely because the human is the control element.

The human control element senses input stimuli such as

- Approach distance
- Incident angle
- Hazards in terrain
and makes decisions regarding any abnormal occurrence of these stimuli. Thus, human controlled corrective action may be taken, such as changes in speed or direction, to prevent an accident.

Most human control actions in transportation systems will be modeled as feedforward control. For example, in the case in which a driver encounters an oncoming car veering left of center, the driver may steer to the extreme right of the road to avoid a collision. Such mitigating action can be modeled as feedforward control since the time and location where an assessment of the hazard was made occurred before the time and location where the accident would have occurred if no mitigating action were employed.

A more complicated feedforward control loop involves considering a train control system with braking and throttling. Consider, for example, the physical terrain in Figure 27 which consists of a valley with a long, initial downhill run followed by an uphill section on the far side of the valley. In the valley (i.e., at the bottom of the hill) there is a curve. When the train goes uphill (with the aft cars going downhill), a centrifugal force at the curve can result in a train derailment if the train is going too fast. Hence, the operator must slow down if he is going too fast. However, if he applies the brakes without applying the throttle simultaneously, an excessive lateral force from the aft cars can cause the car at the bottom of the hill to derail. This is because the brakes cannot be applied simultaneously to all cars. Following this example, the braking line first depressurizes at the engine, subsequently depressurizing the braking system of each car, with an applied-brake interval between the engine and aft cars. Hence, the front cars brake before the rear cars.

The braking and throttling control prevents derailment due to excessive lateral force from the aft cars—shown as the feedforward control in the digraph in Figure 28.

As previously emphasized, the operator is an important control element in transportation systems. In many cases, the time available for an operator to
FIGURE 27
RAILROAD TERRAIN
LATERAL FORCE
AFT CARS

AFT
GRADE
POSITIVE

DECELERATION
THROTTLE

BRAKING
OPERATOR

FIGURE 28
FEED FORWARD CONTROL TO
PREVENT DERAILMENT
respond will determine his effectiveness in preventing accidents. Due to the lack of data, experiments as described for the pressure tank system in Section 2.9 would have to be conducted to obtain data for human responses. Modeling the dynamics of human response will be considered in the following sections, using the digraph fault tree methodology to model and analyze accidents for the marine and rail modes of transportation.

In those sections, we modeled mitigating actions--i.e., control loops--in terms of three time frames, as described in Figure 29. This figure is taken from a report written by Planning Research Corporation for the U.S. Coast Guard.10 "Time frames", a concept used in that report, involves constructing fault trees in the marine mode. We find such a concept directly applicable to generating and analyzing control loops by the digraph-fault tree procedure.

Another concern in obtaining data in transportation risk modeling involves estimating the following conditional probability.

By taking a mitigating feature or equipment failure as the scenario, we ask what is the probability that an accident or potentially serious situation will result? For example, not all blow outs of front tires on vehicles lead to accidents. The fault tree approach involves describing the occurrence of the Top Event, i.e., describing an accident, in terms of its basic events. Not only do we need probabilistic data for these events to find the Top Event probability, but we need, in many cases, the conditional probability described above.
SPILL

OR

COLLISION  RAMMING  GROUNDING

SHORT TIME FRAME CAUSES
THE SITUATION BECOMES EXTREMIS AND THE TIME REMAINING TO TAKE PREVENTIVE MEASURES ARE SUCH THAT AN ACCIDENT IS HIGHLY LIKELY.

INTERMEDIATE TIME FRAME CAUSES/CONTRIBUTING FACTORS
FACTORS COMBINE OR ARE COMPOUNDED TO PRODUCE A POTENTIALLY CRITICAL SITUATION IF THE ERRORS ARE NOT SUCCESSFULLY CORRECTED.

LONG TIME FRAME CONTRIBUTING FACTORS
MISJUDGEMENTS, LESS THAN ADEQUATE CALCULATED RISKS AND OVERSIGHTS INVOLVING NAVIGATION, VESSEL OPERATION, SEAMANSHIP AND/OR GENERAL PRUDENCE THAT CAN LATER PLACE THE VESSEL IN A CRITICAL SITUATION.

FIGURE 29
CONCEPTUAL RELATIONSHIPS OF FAULT TREE TIME CONSIDERATIONS

3-7
4.0 ACCIDENT MODELING AND ANALYSIS FOR THE MARINE MODE

The basic control elements in the marine mode are those that control speed and direction, e.g., engine and steering control. A number of navigational aids exist in preventing collision. These include:

- Maps
- Special radio broadcasts
- Collision avoidance radar
- Flags and lights
- Bells and whistles
- Tugs

Transit of all vessels in U.S. waters are governed by the Coast Guard rules of the road. These rules are very straightforward, e.g., in a meeting situation, vessels pass on the port (left) side. For transit of hazardous cargo such as liquefied natural gas, LNG, and liquefied propane Gas, LPG, special coast guard rules are imposed by the U.S. Coast Guard. One example is Boston Harbor, in which LNG Tankers from Algeria transport LNG through Boston Harbor to the city of Everett where LNG storage tanks are located. (see fig. 30)

As described in the introduction, Barlow and Lambert\(^{4}\) conducted a study to determine the effectiveness of these rules in reducing the probability of LNG-Tanker ship collision. This study used standard fault tree techniques in generating collision scenarios involving an LNG tanker. We in this report will use the digraph-fault tree methodology to generate these scenarios for the marine mode and illustrate how additional insights can be gained using this technique. To accomplish these objectives, we discuss the following topics:

- Special coast guard rules
- System variables for the marine mode
• Dynamics considerations
• System digraph
• Discussion of control loops and loop summaries
• Fault tree construction
• Fault tree evaluation.

4.1 SPECIAL COAST GUARD RULES

The U. S. Coast Guard imposes special rules concerning the transport of LNG within Boston Harbor. These rules are summarized below:

• The maximum allowed speed for the LNG tanker is 8 knots
• No other ship shall be within the "moving safe area" of the LNG tanker defined as 1 nautical mile astern and 2 nautical miles ahead of the tanker
• The Coast Guard broadcasts security announcements every 15 minutes on channels 13 FM and 16 FM
• Transit is during daylight hours with 2 miles visibility
• The LNG tanker is accompanied by 3 tugs and Coast Guard escort

If any ship attempts to enter the moving safe area and is sited by either the escort or a cruising coast guard cutter, then this ship will be ordered to dock. The above rules will serve as initial conditions to the digraph-fault tree analyses.

The Top Event of interest is "LNG Tanker - Ship Collision Causes Release of LNG."

4.2 SYSTEM VARIABLES FOR THE MARINE MODE

We must define variable relationships necessary in describing collision between the LNG tanker and a potential striking vessel in the harbor.
Important system variables include:

- Speed of both ships, \( V_1 \) and \( V_2 \)
- Distance between ships
- Incident angle \( \theta_L \) at distance \( L \) (see fig. 31)

Subscript 1 refers to the LNG tanker and subscript 2 refers to the potential striking vessel. The concept of moving safe area suggests that distance between two ships is an important variable and will be used in this study.

It is proposed to introduce the concept of critical area defined as an area in which if occupied by two ships, the possibility of collision is great.

In order that collision occur, the following sequence of events must occur.

1. Potential striking vessel enters moving safe area of LNG Tanker
2. Equipment failure or human error cause the potential striking vessel to be on a collision course in the moving safe area
3. Ship enters critical area and collision results

4.3 DYNAMICS CONSIDERATIONS

We will structure the control loads in the digraph in the same method fault trees were constructed in fig. 29 using timing considerations.

- Ships outside the moving safe area have adequate time for communications and navigation. Errors in judgment, equipment failure, weather conditions or in combination permit the ship to enter the moving safe area.
- Dynamics of human response in the moving safe area are important but not as important as in the critical area. In the moving safe area, assessment of approach angle and distance are made. Communications are important.
CONCEPT OF CRITICAL AREA
In the critical area, immediate action is required to avoid a potential collision (i.e. collision becomes imminent) characteristics of the critical area are:

- Human error rates are higher when both ships occupy this area due to the possibility of collision
- Communications are ineffective in preventing collision
- Immediate maneuvering actions such as steering and changing engine speed are required in preventing collision.

### 4.4 SYSTEM DIGRAPH

A system digraph shown in fig. 32 with Top Event, "Collision with Release." The important variables nodes presented below cause the collision to occur.

<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Collision with release</td>
</tr>
<tr>
<td>27</td>
<td>Critical velocity and angle exceeded at impact</td>
</tr>
<tr>
<td>22</td>
<td>Collision</td>
</tr>
<tr>
<td>29</td>
<td>On collision course in critical area</td>
</tr>
<tr>
<td>21</td>
<td>Ship in critical area</td>
</tr>
<tr>
<td>3</td>
<td>Ship in moving safe area</td>
</tr>
<tr>
<td>15 (and all input nodes)</td>
<td>Loss of ship control</td>
</tr>
<tr>
<td>18 (and all input nodes)</td>
<td>Loss of LNG tanker control</td>
</tr>
<tr>
<td>2</td>
<td>LNG Tanker transiting Boston Harbor</td>
</tr>
<tr>
<td>1</td>
<td>Ship transiting Boston Harbor</td>
</tr>
</tbody>
</table>
These nodes will appear on causative branches of NFFL's.

As we follow the above sets of nodes from 1 to 28 on the digraph, we see that the sequences of events as described in section 4.2 must occur for collision. Also note that as one proceeds from node 1 to 28, the distance between the two ships decrease. The two ships are close enough that the variables, speed and direction, become important in the moving safe area. As shown in the digraph on Fig. 32, loss of steering or engine control on either ship can cause the potential striking vessel to occupy the critical area. Note that a ship in the moving safe area does not imply collision. Normally, ships with non-hazardous cargo may pass within 50 feet of each other in the harbor, a distance well within the moving safe area.

4.5 CONTROL LOOPS

As the ship attempts to enter the moving safe area, a series of mitigating actions, (NFFL's as shown in Fig. 32), may be employed in preventing the ship's movement into this area. Upon visual siting of either the ship or LNG Tanker, communications can be made in preventing the ship from occupying the moving safe area. In addition, the coast guard siting of the ship in the harbor can result in orders from the Coast Guard for the ship to dock.

These loops are also effective in the moving safe area (for sake of space, these loops are not repeated in fig. 32 but are described in Table one). In the critical area, where dynamics are important, two loops exist in preventing collision. Either the captain of the LNG tanker or ship, through steering or engine control, can take immediate remedial action in preventing a collision.

Table one gives a summary of the NFFL's shown in Figure 32. Nodes for both the causative and corrective branches are shown. Events which inactivate loops are shown. The last column gives consideration to dynamics.
### Table 1
SUMMARY OF NEGATIVE FEEDBACK LOOPS FOR RELEASE OF LNG IN BOSTON HARBOR DUE TO LNG TANKER-SHIP COLLISION

#### Negative Feed Forward Loop

<table>
<thead>
<tr>
<th>Area</th>
<th>NFFL No.</th>
<th>Description</th>
<th>Nodes for Causative Branch</th>
<th>Nodes for Corrective Branch</th>
<th>Inactivation Events</th>
<th>Dynamics Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>1</td>
<td>Ship senses LNG tanker on radar and does not enter moving safe area (or critical area)</td>
<td>2-3</td>
<td>2-4-5-3</td>
<td>1. Ship radar turned off</td>
<td>important in moving safe area</td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>2</td>
<td>Ship sites LNG tanker visually and does not enter or moving safe area (or critical area)</td>
<td>2-3</td>
<td>2-6-5-3</td>
<td>1. Bad weather</td>
<td>important in moving area</td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>3</td>
<td>Ship receives Coast Guard broadcast and does not enter moving safe area (or critical area)</td>
<td>1-2-3</td>
<td>1-7-3</td>
<td>1. Ship radio turned off</td>
<td>important in moving safe area</td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>4</td>
<td>Cruising Coast Guard Cutter orders ship to dock</td>
<td>1-2-3</td>
<td>1-8-9-3</td>
<td>1. Bad weather</td>
<td>important in moving safe area</td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>5</td>
<td>Ship hears whistles on LNG Tanker and does not enter moving safe area (or critical area)</td>
<td>1-2-3</td>
<td>1-11-12-13-5-3</td>
<td>1. Bad weather</td>
<td>important in moving safe area</td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>6</td>
<td>'options remain blank for in critical area'</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Outside Moving Safe Area</strong></td>
<td>7</td>
<td>Ship hears radio broadcast from LNG tanker and does not enter moving safe area</td>
<td>1-2-3</td>
<td>1-11-12-14-5-3</td>
<td>1. Bad weather</td>
<td>important in moving safe area</td>
</tr>
<tr>
<td><strong>In Critical Area</strong></td>
<td>9</td>
<td>Ship captain's action avoids collision with LNG Tanker</td>
<td>21-22</td>
<td>21-23-24-22</td>
<td>1. Ship speed too fast</td>
<td>extremely important</td>
</tr>
<tr>
<td><strong>In Critical Area</strong></td>
<td>10</td>
<td>LNG captain's action avoid collision with ship</td>
<td>21-22</td>
<td>21-25-26-22</td>
<td>1. LNG Tanker speed too fast</td>
<td>extremely important</td>
</tr>
</tbody>
</table>
4.6 FAULT TREE CONSTRUCTION

The fault tree constructed from the digraph in fig. 32 is shown in fig. 33. Basic event and gate names with eight characters or less represent alphanumeric names in the computer analysis. The fault tree was constructed by use of the synthesis algorithm described in section 2.9. The negative feed forward loop operator in fig. 20 was successively used successively many times. The trigger nodes (as described in section 2.9) which generates AND gates are nodes 2, 3 and 22 in fig. 32. All causative branches of the NFFL's in fig. 32 contain two nodes with a conditional edge statement. Hence, the trigger node for all NFFL's occurs at the end of the negative feed forward loop.

4.7 FAULT TREE EVALUATION

The collision scenarios were generated by finding the min cut sets to the fault tree in fig. 33. A total of 3840 min cut sets were found that ranged in length from 10 basic events to 11 basic events. The min cut sets were found by the use of the computer code FTAP.\(^{(12)}\)

The fault tree was quantified using the following data for the basic events

<table>
<thead>
<tr>
<th>BASIC EVENT TYPE</th>
<th>PROBABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment failure</td>
<td>(1.6 \times 10^{-5}/\text{transit})</td>
</tr>
<tr>
<td>Human error</td>
<td>(10^{-1}) to (10^{-2}/\text{event})</td>
</tr>
<tr>
<td>Bad weather developing in transit</td>
<td>(2 \times 10^{-2}/\text{transit})</td>
</tr>
<tr>
<td>Critical angle and velocity exceeded at impact causing release</td>
<td>(1.6 \times 10^{-2})</td>
</tr>
</tbody>
</table>
Collision with Release AND

Critical Angle and Velocity Exceeded at Impact (CRITANVE)

Collision (G1)

Ship's captain action fails to avoid collision with LNG Tanker and LNG captain's action fails to avoid collision with ship when ship is in Critical Area (G2)

Human Error or Equipment causes ship to be on collision course with LNG tanker (COLUSION)

Ship's captain action fails to avoid collision with LNG Tanker, i.e. NFFL #9 fails (G3)

Ship speed too fast (SHIPSPEE)

No or slow response from ship (SHIPNOR)

Loss of ship steering CONTROL (G6)

Loss of ship engine control

Loss of Speed Control on LNG Tanker (G7)

LNG Tanker's action fails to avoid collision with ship, i.e. NFFL #10 fails (G5)

LNG Tanker's speed too FAST (LNGSPEED)

No or slow response from LNG Tanker (LNGNOR)

Fault Tree for Release of LNG in Boston Harbor Due to LNG Tanker-Ship Collision

Sheet 1
(G4) Ship in critical Area

OR

Loss of Ship control while ship in moving (G10) safe area

AND

Loss of ship control (G11)

Loss of ship steering control (G6)

Loss of ship steering control equipment failure (SPSTEG)

Loss of ship steering control human error (SPSTHE)

Loss of ship engine control (G7)

Loss of ship engine control equipment failure (SPENEQ)

Loss of ship engine control human error (SPENHE)

Ship in moving safe area (G13)

Ship in moving safe area (G13)

Loss of LNG Tanker Steering Control equipment failure (LNGSTEG)

Loss of LNG Tanker Steering Control human error (LNGSTHE)

Loss of LNG Tanker Engine Control equipment failure (LNGENEQ)

Loss of LNG Tanker Engine Control human error (LNGENHE)

FIGURE 33 (CONT.)

SHEET 2
Ships radar (G15) fails to sense LNG tanker and enters moving safe area, i.e., NFFL#1 fails Q/R 1. Ship radar turned off (SPRDOFF) 2. Ship radar ignored (SPRDIGN) 3. Ship has no radar (SPNORAD)
5.0 REFERENCES


3. H. E. Lambert, J. J. Lim and F. M. Gilman, A Digraph - Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Calif., UCRL 52710 (May 1979).*


8. H. E. Lambert, J. J. Lim and F. M. Gilman, A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Rept. UCRL-52170 (1979).*


* Available from National Technical Information Service; Springfield, VA. 22151, USA.


* Available from National Technical Information Service; Springfield, VA. 22151, USA.
APPENDIX A

GLOSSARY OF TERMS USED IN THE LAPP-POWERS FAULT TREE SYNTHESIS ALGORITHM

1. **Digraph**: Nodes connected by edges which have direction.

2. **Edge**: The line connecting two nodes. It indicates a relationship between the two nodes. The number next to the edge is the gain = Δ output/Δ input.

3. **Conditional Edge**: The relationship between two nodes depends on another event or variable, i.e. The gain between valve position and flow out of the valve is zero if the valve is stuck. The conditional statement is "valve stuck."

4. **Primal Node**: A node on the system digraph with no inputs.

5. **Input**: The node(s) whose edges point to the node under consideration.

6. **Local Input**: Variables or events one node away from the node being considered.

7. **Gain**: Change in Output/change in Input. Gains may have values of ±10, ±1, 0. Zero means no gain or relationship.

8. **Variable and Event Values**: ±10, ±1, 0. These are deviations of the variables and events from their normal value. ±10 indicates large deviations which cannot be handled by normal NFBL. ±1 is the usual deviation expected in the variable or event. Zero means no deviation. Some variables are univariant (can only vary in one direction from their normal value) i.e. A normally open valve cannot be further opened: A fire can only have values of 0, ±1, and ±10.

9. **Feedback Loop (FBL)**: A path through nodes in the digraph which starts and terminates at one node.
10. Negative Feedback Loop (NFBL): A feedback loop in which the product of the normal gains around the loop is negative.

11. Positive Feedback Loop (PFBL): The product of the gains around the FBL is positive.

12. Feedforward Loop (FFL): Two or more paths from one node in a digraph to another different node in the digraph.

13. Negative Feedforward Loop (NFFL): A FFL in which the sign of the product of the normal gains of one of the branches of the FFL is different from the others.

14. Variables Just before the Start of NFFL:

15. Inactive: Gain of zero between the two nodes.
3.0 TRANSPORTATION RISK MODELING

A concern of the Department of Transportation, DOT, involves the transportation of hazardous materials, such as radioactive waste and chemical substances. DOT is interested in choosing routes which will minimize the risk in transporting these materials. Unfortunately, only nationwide accident event rates exist and are not available for individual routes. One purpose of this report is to present a methodology allowing DOT to choose a route which will minimize the risk.

The approach centers around two steps:

- Devise a methodology capable of generating accident scenarios in terms of basic events in which data exists or can be obtained
- Devise an approach to obtain data for basic events in which data does not exist

Dynamics and the human control elements are important considerations in transportation systems, as well as terrain, traffic frequency and environmental conditions. We feel that the digraph-fault tree methodology can address these considerations as well as generate meaningful scenarios which can be analyzed for assessment of routes.

A transportation system is a control system with accident mitigating features, such as braking, navigation and steering systems.

The differences between modeling a chemical processing system and a transportation system as a controlled system are:

- Definition of the system
- System variables

A chemical processing system is a well defined system with inputs, outputs and means of control clearly delineated. In a transportation system, variables are
always changing—variables such as distance, approach angle and velocity. Depending upon each value of these variables, means of control may be different, e.g., braking or acceleration. These factors must be included when defining a transportation system and in constructing a digraph for the system.

Modeling a transportation system as a control system, while using the digraph-fault tree methodology, requires the following topics to be addressed:

- Define variables in transportation systems
- Model control in transportation systems as feedback and feedforward control
- Incorporation of dynamics

Because system variables change in transportation systems, the "normal" value, i.e., the "0" value, also changes. Hence, it is important to make system variables location specific, and define these variables in terms of each system's environmental conditions, e.g., weather, grade, frequency of traffic, etc. The effectiveness of accident mitigating systems changes with each change in condition. A case in point is a wet railroad track.

The next consideration is the modeling of control loops in transportation systems. Many automatic controls do exist in transportation systems; and these systems can be modeled exactly the same way that chemical control systems were in the previous section. Many control loops exist precisely because the human is the control element.

The human control element senses input stimuli such as

- Approach distance
- Incident angle
- Hazards in terrain
and makes decisions regarding any abnormal occurrence of these stimuli. Thus, human controlled corrective action may be taken, such as changes in speed or direction, to prevent an accident.

Most human control actions in transportation systems will be modeled as feedforward control. For example, in the case in which a driver encounters an oncoming car veering left of center, the driver may steer to the extreme right of the road to avoid a collision. Such mitigating action can be modeled as feedforward control since the time and location where an assessment of the hazard was made occurred before the time and location where the accident would have occurred if no mitigating action were employed.

A more complicated feedforward control loop involves considering a train control system with braking and throttling. Consider, for example, the physical terrain in Figure 27 which consists of a valley with a long, initial downhill run followed by an uphill section on the far side of the valley. In the valley (i.e., at the bottom of the hill) there is a curve. When the train goes uphill (with the aft cars going downhill), a centrifugal force at the curve can result in a train derailment if the train is going too fast. Hence, the operator must slow down if he is going too fast. However, if he applies the brakes without applying the throttle simultaneously, an excessive lateral force from the aft cars can cause the car at the bottom of the hill to derail. This is because the brakes cannot be applied simultaneously to all cars. Following this example, the braking line first depressurizes at the engine, subsequently depressurizing the braking system of each car, with an applied-brake interval between the engine and aft cars. Hence, the front cars brake before the rear cars.

The braking and throttling control prevents derailment due to excessive lateral force from the aft cars—shown as the feedforward control in the digraph in Figure 28.

As previously emphasized, the operator is an important control element in transportation systems. In many cases, the time available for an operator to
LATERAL FORCE AFT CARS

AFT GRADE + POSITIVE

DECELERATION + BRAKING +

OPERATOR

THROTTLE -

FIGURE 28
FEED FORWARD CONTROL TO PREVENT DERAILMENT
respond will determine his effectiveness in preventing accidents. Due to the lack of data, experiments as described for the pressure tank system in Section 2.9 would have to be conducted to obtain data for human responses. Modeling the dynamics of human response will be considered in the following sections, using the digraph fault tree methodology to model and analyze accidents for the marine and rail modes of transportation.

In those sections, we modeled mitigating actions--i.e., control loops--in terms of three time frames, as described in Figure 29. This figure is taken from a report written by Planning Research Corporation for the U.S. Coast Guard. "Time frames", a concept used in that report, involves constructing fault trees in the marine mode. We find such a concept directly applicable to generating and analyzing control loops by the digraph-fault tree procedure.

Another concern in obtaining data in transportation risk modeling involves estimating the following conditional probability.

By taking a mitigating feature or equipment failure as the scenario, we ask what is the probability that an accident or potentially serious situation will result? For example, not all blow outs of front tires on vehicles lead to accidents. The fault tree approach involves describing the occurrence of the Top Event, i.e., describing an accident, in terms of its basic events. Not only do we need probabilistic data for these events to find the Top Event probability, but we need, in many cases, the conditional probability described above.
SPILL

OR

COLLISION  RAMMING  GROUNDING

SHORT TIME FRAME CAUSES
THE SITUATION BECOMES EXTREMIS AND THE TIME REMAINING TO TAKE PREVENTIVE MEASURES ARE SUCH THAT AN ACCIDENT IS HIGHLY LIKELY.

INTERMEDIATE TIME FRAME CAUSES/CONTRIBUTING FACTORS
FACTORS COMBINE OR ARE COMPOUNDED TO PRODUCE A POTENTIALLY CRITICAL SITUATION IF THE ERRORS ARE NOT SUCCESSFULLY CORRECTED.

LONG TIME FRAME CONTRIBUTING FACTORS
MISJUDGEMENTS, LESS THAN ADEQUATE CALCULATED RISKS AND OVERSIGHTS INVOLVING NAVIGATION, VESSEL OPERATION, SEAMANSHIP AND/OR GENERAL PRUDENCE THAT CAN LATER PLACE THE VESSEL IN A CRITICAL SITUATION.

FIGURE 29
CONCEPTUAL RELATIONSHIPS OF FAULT TREE TIME CONSIDERATIONS
4.0 ACCIDENT MODELING AND ANALYSIS FOR THE MARINE MODE

The basic control elements in the marine mode are those that control speed and direction, e.g., engine and steering control. A number of navigational aids exist in preventing collision. These include:

- Maps
- Special radio broadcasts
- Collision avoidance radar
- Flags and lights
- Bells and whistles
- Tugs

Transit of all vessels in U.S. waters are governed by the Coast Guard rules of the road. These rules are very straightforward, e.g., in a meeting situation, vessels pass on the port (left) side. For transit of hazardous cargo such as liquefied natural gas, LNG, and liquefied propane gas, LPG, special coast guard rules are imposed by the U.S. Coast Guard. One example is Boston Harbor, in which LNG tankers from Algeria transport LNG through Boston Harbor to the city of Everett where LNG storage tanks are located. (see fig. 30)

As described in the introduction, Barlow and Lambert\(^4\) conducted a study to determine the effectiveness of these rules in reducing the probability of LNG-Tanker ship collision. This study used standard fault tree techniques in generating collision scenarios involving an LNG tanker. We in this report will use the digraph-fault tree methodology to generate these scenarios for the marine mode and illustrate how additional insights can be gained using this technique. To accomplish these objectives, we discuss the following topics:

- Special coast guard rules
- System variables for the marine mode
• Dynamics considerations
• System digraph
• Discussion of control loops and loop summaries
• Fault tree construction
• Fault tree evaluation.

4.1 SPECIAL COAST GUARD RULES

The U. S. Coast Guard imposes special rules concerning the transport of LNG within Boston Harbor. These rules are summarized below:

• The maximum allowed speed for the LNG tanker is 8 knots
• No other ship shall be within the "moving safe area" of the LNG tanker defined as 1 nautical mile astern and 2 nautical miles ahead of the tanker
• The Coast Guard broadcasts security announcements every 15 minutes on channels 13 FM and 16 FM
• Transit is during daylight hours with 2 miles visibility
• The LNG tanker is accompanied by 3 tugs and Coast Guard escort

If any ship attempts to enter the moving safe area and is sited by either the escort or a cruising coast guard cutter, then this ship will be ordered to dock. The above rules will serve as initial conditions to the digraph-fault tree analyses.

The Top Event of interest is "LNG Tanker - Ship Collision Causes Release of LNG."

4.2 SYSTEM VARIABLES FOR THE MARINE MODE

We must define variable relationships necessary in describing collision between the LNG tanker and a potential striking vessel in the harbor.
Important system variables include:

- Speed of both ships, $V_1$ and $V_2$
- Distance between ships
- Incident angle $\theta_L$ at distance $L$ (see fig. 31)

Subscript 1 refers to the LNG tanker and subscript 2 refers to the potential striking vessel. The concept of moving safe area suggests that distance between two ships is an important variable and will be used in this study.

It is proposed to introduce the concept of critical area defined as an area in which if occupied by two ships, the possibility of collision is great.

In order that collision occur, the following sequence of events must occur.

1. Potential striking vessel enters moving safe area of LNG Tanker
2. Equipment failure or human error cause the potential striking vessel to be on a collision course in the moving safe area
3. Ship enters critical area and collision results

4.3 DYNAMICS CONSIDERATIONS

We will structure the control loads in the digraph in the same method fault trees were constructed in fig. 29 using timing considerations.

- Ships outside the moving safe area have adequate time for communications and navigation. Errors in judgment, equipment failure, weather conditions or in combination permit the ship to enter the moving safe area.
- Dynamics of human response in the moving safe area are important but not as important as in the critical area. In the moving safe area, assessment of approach angle and distance are made. Communications are important.
FIGURE 31

CONCEPT OF CRITICAL AREA
In the critical area, immediate action is required to avoid a potential collision (i.e. collision becomes imminent) characteristics of the critical area are:

- Human error rates are higher when both ships occupy this area due to the possibility of collision
- Communications are ineffective in preventing collision
- Immediate maneuvering actions such as steering and changing engine speed are required in preventing collision.

### 4.4 SYSTEM DIGRAMH

A system digraph shown in fig. 32 with Top Event, "Collision with Release." The important variables nodes presented below cause the collision to occur

<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Collision with release</td>
</tr>
<tr>
<td>27</td>
<td>Critical velocity and angle exceeded at impact</td>
</tr>
<tr>
<td>22</td>
<td>Collision</td>
</tr>
<tr>
<td>29</td>
<td>On collision course in critical area</td>
</tr>
<tr>
<td>21</td>
<td>Ship in critical area</td>
</tr>
<tr>
<td>3</td>
<td>Ship in moving safe area</td>
</tr>
<tr>
<td>15</td>
<td>Loss of ship control</td>
</tr>
<tr>
<td>18</td>
<td>Loss of LNG tanker control</td>
</tr>
<tr>
<td>2</td>
<td>LNG Tanker transiting Boston Harbor</td>
</tr>
<tr>
<td>1</td>
<td>Ship transiting Boston Harbor</td>
</tr>
</tbody>
</table>
FIGURE 32
DIGRAPH FOR RELEASE OF LNG IN BOSTON HARBOR DUE TO LNG Tanker-Ship Collision

- Ship's captain action in critical area
- Control of ship in critical area
- Near slow response
- Critical speed
- Control of LNG tanker in critical area
- On collision course in critical area
- LNG captain's action in critical area
- Human error
- Equipment failure
- Loss of steering control (ship)
- Loss of control (ship)
- Loss of engine control (ship)
- Loss of control (LNG tanker)
- Loss of steering (LNG tanker)
- Loss of engine control (LNG tanker)
- Cruising Coast Guard orders ship to dock
- Ship transiting Boston Harbor
- LNG tanker transiting Boston Harbor
- Ship radar indication
- Ship radar broadcast received
- Coast Guard visual siting of ship
- LNG Tanker sights ship
- LNG Tanker radar indication of ship
- Radio failure on LNG Tanker
- Whistles on LNG Tanker not sounded
These nodes will appear on causative branches of NFFL's.

As we follow the above sets of nodes from 1 to 28 on the digraph, we see that the sequences of events as described in section 4.2 must occur for collision. Also note that as one proceeds from node 1 to 28, the distance between the two ships decrease. The two ships are close enough that the variables, speed and direction, become important in the moving safe area. As shown in the digraph on Fig. 32, loss of steering or engine control on either ship can cause the potential striking vessel to occupy the critical area. Note that a ship in the moving safe area does not imply collision. Normally, ships with non-hazardous cargo may pass within 50 feet of each other in the harbor, a distance well within the moving safe area.

4.5 CONTROL LOOPS

As the ship attempts to enter the moving safe area, a series of mitigating actions, (NFFL's as shown in Fig. 32), may be employed in preventing the ship's movement into this area. Upon visual siting of either the ship or LNG Tanker, communications can be made in preventing the ship from occupying the moving safe area. In addition, the coast guard siting of the ship in the harbor can result in orders from the Coast Guard for the ship to dock.

These loops are also effective in the moving safe area (for sake of space, these loops are not repeated in fig. 32 but are described in Table one). In the critical area, where dynamics are important, two loops exist in preventing collision. Either the captain of the LNG tanker or ship, through steering or engine control, can take immediate remedial action in preventing a collision.

Table one gives a summary of the NFFL's shown in Figure 32. Nodes for both the causative and corrective branches are shown. Events which inactivate loops are shown. The last column gives consideration to dynamics.
<table>
<thead>
<tr>
<th>Area</th>
<th>NFFL No.</th>
<th>Description</th>
<th>Nodes for Causative Branch</th>
<th>Nodes for Corrective Branch</th>
<th>Inactivation Events</th>
<th>Dynamics Consideration</th>
</tr>
</thead>
</table>
| Outside Moving                   | 1        | Ship senses LNG tanker on radar and does not enter moving safe area (or critical area) | 2-3                        | 2-4-5-3                      | 1. Ship radar turned off  
2. Ship radar ignored  
3. Ship has no radar  | important in moving safe area    |
| Safe Area & Inside               |          |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| Outside Moving                   | 2        | Ship sites LNG tanker visually and does not enter or moving safe area (or critical area) | 2-3                        | 2-6-5-3                      | 1. Bad weather  
2. Human error on ship, no visual siting | important in moving safe area    |
| Safe Area & Inside               |          |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| Outside Moving                   | 3        | Ship receives Coast Guard broadcast and does not enter moving safe area (or critical area) | 1-2-3                      | 1-7-3                        | 1. Ship radio turned off  
2. Coast Guard fails to give early warning  
3. Nonadherence to Coast Guard broadcast  
4. Human error on ship does not listen to broadcast | important in moving safe area    |
| Safe Area & Inside               |          |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| Outside Moving                   | 4        | Cruising Coast Guard Cutter orders ship to dock                            | 1-2-3                      | 1-8-9-3                      | 1. Bad weather  
2. Coast Guard cutter unavailable | important in moving safe area    |
| Safe Area & Inside               |          |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| Outside Moving                   | 5        | Ship hears whistles on LNG Tanker and does not enter moving safe area (or critical area) | 1-2-3                      | 1-11-12-13-5-3               | 1. Bad weather  
2. Whistles on LNG tanker not sounded  
3. LNG Tanker whistles not heard by ship (human error)  
1. LNG Tanker radar turned off  
2. Whistles on LNG Tanker not sounded  
3. LNG Tanker whistles not heard by ship (human error)  
4. LNG Tanker radar ignored | important in moving safe area    |
| Safe Area & Inside               | 6        |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| Outside Moving                   | 7        | Ship hears radio broadcast from LNG tanker and does not enter moving safe area | 1-2-3                      | 1-11-12-14-5-3               | 1. Bad weather  
2. Radio Failure on LNG Tanker  
3. Human error in listening to LNG Tanker radio message  
1. LNG Tanker Radar turned off  
2. LNG Tanker radar ignored  
3. Radio failure on LNG Tanker  
4. Human error in listening to LNG Tanker radio message | important in moving safe area    |
| Safe Area & Inside               | 8        |                                                                            |                            |                              |                                                                                      |                                          |
| Moving Safe Area                 |          |                                                                            |                            |                              |                                                                                      |                                          |
| In Critical Area                 | 9        | Ship captain's action avoids collision with LNG Tanker                       | 21-22                      | 21-23-24-22                  | 1. Ship speed too fast  
2. No or slow response from ship  
3. Loss of ship steering  
4. Loss of ship engine control | extremely important             |
| In Critical Area                 | 10       | LNG captain's action avoid collision with ship                              | 21-22                      | 21-25-26-22                  | 1. LNG Tanker speed too fast  
2. No or slow response from LNG Tanker  
3. Loss of steering control on LNG tanker  
4. Loss of engine control on LNG tanker | extremely important             |
4.6 FAULT TREE CONSTRUCTION

The fault tree constructed from the digraph in fig. 32 is shown in fig. 33. Basic event and gate names with eight characters or less represent alphanumeric names in the computer analysis. The fault tree was constructed by use of the synthesis algorithm described in section 2.9. The negative feed forward loop operator in fig. 20 was successively used successively many times. The trigger nodes (as described in section 2.9) which generates AND gates are nodes 2, 3 and 22 in fig. 32. All causative branches of the NFFL's in fig. 32 contain two nodes with a conditional edge statement. Hence, the trigger node for all NFFL's occurs at the end of the negative feed forward loop.

4.7 FAULT TREE EVALUATION

The collision scenarios were generated by finding the min cut sets to the fault tree in fig. 33. A total of 3840 min cut sets were found that ranged in length from 10 basic events to 11 basic events. The min cut sets were found by the use of the computer code FTAP.(12)

The fault tree was quantified using the following data for the basic events

<table>
<thead>
<tr>
<th>BASIC EVENT TYPE</th>
<th>PROBABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment failure</td>
<td>$1.6 \times 10^{-5}$/transit</td>
</tr>
<tr>
<td>Human error</td>
<td>$10^{-1}$ to $10^{-2}$/event</td>
</tr>
<tr>
<td>Bad weather developing in transit</td>
<td>$2 \times 10^{-2}$/transit</td>
</tr>
<tr>
<td>Critical angle and velocity exceeded at impact causing release</td>
<td>$1.6 \times 10^{-2}$</td>
</tr>
</tbody>
</table>
Fault Tree for Release of LNG in Boston Harbor Due to LNG Tanker-Ship Collision

Sheet 1
(G4) Ship in critical Area

OR

Loss of Ship control while ship in moving (G10)
safe area

AND

Loss of ship control (G11)

OR

Loss of ship steering control (G6)

OR

Loss of ship steering control equipment failure (SPSTEQ)

Loss of ship steering control human error (SPSTHE)

Loss of ship engine control (G7)

Loss of ship engine control equipment failure (SPENEQ)

Loss of ship engine control human error (SPENHE)

Ship in moving safe area (G13)

Loss of LNG Control (G12)

Loss of LNG Tanker Steering Control (G9)

Loss of LNG Tanker Steering Control equipment failure (LNGSTEQ)

Loss of LNG Tanker Steering Control human error (LNGSTHE)

Loss of LNG Tanker engine control (G8)

Loss of LNG Tanker engine control equipment failure (LNGENEQ)

Loss of LNG Tanker engine control human error (LNGENHE)
<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFFL’s fail (G14) permitting ship to enter moving safe area AND</td>
<td>LNG Tanker transiting Boston Harbor (LNGTANKR)</td>
<td></td>
</tr>
<tr>
<td>Ships radar (G15) fails to sense LNG Tanker and enters moving safe area, L.E., NFFL#1 fails OR</td>
<td>1. Ship radar turned off (SPRDOFF)</td>
<td></td>
</tr>
<tr>
<td>2. ship radar ignored (SPRDIGN)</td>
<td>3. ship has no radar (SPNORAD)</td>
<td></td>
</tr>
<tr>
<td>Ship (G16) fails to sight LNG Tanker and enters moving safe area, i.e., NFFL#2 fails OR</td>
<td>1. Bad weather (BADWEAR)</td>
<td></td>
</tr>
<tr>
<td>2. No visual sighting on ship due to human error (SPNOSITE)</td>
<td>3. Nonadherence to Coast Guard broadcast (NONADHER)</td>
<td></td>
</tr>
<tr>
<td>4. Ship does not listen to broadcast due to human error (SPNOLIST)</td>
<td>5. LNG Tanker radar turned off (LNRDUFF)</td>
<td></td>
</tr>
<tr>
<td>Ship (G17) fails to receive Coast Guard Broadcast and enters moving safe area, i.e., NFFL#3 fails OR</td>
<td>1. Whistles not sounded on LNG Tanker (LNNOWWHIS)</td>
<td></td>
</tr>
<tr>
<td>2. LNG Tanker whistles not heard by ship (LNWHISHX)</td>
<td>3. Radio ignored LNG Tanker (LNRADHE)</td>
<td></td>
</tr>
<tr>
<td>Ship (G19) fails to hear whistles on LNG Tanker and enters moving safe area (visual sighting) NFFL #5 fails OR</td>
<td>1. Radio Failure on LNG Tanker (LNRAD)</td>
<td></td>
</tr>
<tr>
<td>2. Human error in listening to radio message from LNG tanker (LNRADHE)</td>
<td>3. Radionics failure on LNG Tanker (LNRADICS)</td>
<td></td>
</tr>
<tr>
<td>Ship (G20) fails to hear radio broadcast from LNG tanker and enters moving safe area (radar) NFFL #6 fails OR</td>
<td>1. Bad Weather (BADWEAR)</td>
<td></td>
</tr>
<tr>
<td>2. Whistles on LNG Tanker not sounded (LNNOWWHIS)</td>
<td>3. Human error in listening to radio message from LNG tanker (LNRADHE)</td>
<td></td>
</tr>
<tr>
<td>4. Human error in listening to radio message from LNG tanker (LNRADHE)</td>
<td>5. Radionics failure on LNG Tanker (LNRADICS)</td>
<td></td>
</tr>
<tr>
<td>Ship (G21) fails to hear radio broadcast from LNG tanker and enters moving safe area (radar) NFFL #8 fails OR</td>
<td>1. LNG Tanker radar turned off (LNRDUFF)</td>
<td></td>
</tr>
<tr>
<td>2. LNG Tanker radar ignored (LNRDIGN)</td>
<td>3. Radio Failure on LNG Tanker (LNRAD)</td>
<td></td>
</tr>
<tr>
<td>4. Human error in listening to radio message from LNG tanker (LNRADHE)</td>
<td>6. Radionics failure on LNG Tanker (LNRADICS)</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 33 (Cont.)**
5.0 REFERENCES


3. H. E. Lambert, J. J. Lim and F. M. Gilman, A Digraph - Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Calif., UCRL 52170 (May 1979).*


8. H. E. Lambert, J. J. Lim and F. M. Gilman, A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Rept. UCRL-52170 (1979).*


* Available from National Technical Information Service; Springfield, VA. 22151, USA.


* Available from National Technical Information Service; Springfield, VA. 22151, USA.
APPENDIX A

GLOSSARY OF TERMS USED IN THE LAPP-POWERS FAULT TREE SYNTHESIS ALGORITHM

1. Digraph: Nodes connected by edges which have direction.

2. Edge: The line connecting two nodes. It indicates a relationship between the two nodes. The number next to the edge is the gain = \( \frac{\Delta \text{output}}{\Delta \text{input}} \).

3. Conditional Edge: The relationship between two nodes depends on another event or variable, i.e. The gain between valve position and flow out of the valve is zero if the valve is stuck. The conditional statement is "valve stuck."

4. Primal Node: A node on the system digraph with no inputs.

5. Input: The node(s) whose edges point to the node under consideration.

6. Local Input: Variables or events one node away from the node being considered.

7. Gain: Change in Output/change in Input. Gains may have values of \( \pm 10, \pm 1, 0 \). Zero means no gain or relationship.

8. Variable and Event Values: \( \pm 10, \pm 1, 0 \). These are deviations of the variables and events from their normal value. \( \pm 10 \) indicates large deviations which cannot be handled by normal NFBL. \( \pm 1 \) is the usual deviation expected in the variable or event. Zero means no deviation. Some variables are univariant (can only vary in one direction from their normal value) i.e. A normally open valve cannot be further opened: A fire can only have values of 0, +1, and +10.

9. Feedback Loop (FBL): A path through nodes in the digraph which starts and terminates at one node.
10. Negative Feedback Loop (NFBL): A feedback loop in which the product of the normal gains around the loop is negative.

11. Positive Feedback Loop (PFBL): The product of the gains around the FBL is positive.

12. Feedforward Loop (FFL): Two or more paths from one node in a digraph to another different node in the digraph.

13. Negative Feedforward Loop (NFFL): A FFL in which the sign of the product of the normal gains of one of the branches of the FFL is different from the others.

14. Variables Just before the Start of NFFL:

15. Inactive: Gain of zero between the two nodes.