Apr 1st, 8:00 AM

Application of Reliability and System Safety Analytical Techniques to a Civic Need

Thomas G. Goss
Manager Reliability & System Safety Engineering, The Boeing Company

Follow this and additional works at: https://commons.erau.edu/space-congress-proceedings

Scholarly Commons Citation
https://commons.erau.edu/space-congress-proceedings/proceedings-1971-8th/session-13/2

This Event is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in The Space Congress Proceedings by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu, wolfe.309@erau.edu.
APPLICATION OF
RELIABILITY AND SYSTEM SAFETY
ANALYTICAL TECHNIQUES TO A CIVIC NEED

Thomas G. Goss
Manager Reliability &
System Safety Engineering
The Boeing Company
Cocoa Beach, Florida

ABSTRACT
Many billions of tax payer dollars have been
spent on aerospace programs. In order to con­
tinue further expenditures for the exploration of
space, the American people demand a payoff which
is beneficial to the average citizen. This paper
will outline one such "spin-off"; VIZ, the appli­
cation of reliability and system safety analyt­
cal techniques to a civic need.

INTRODUCTION
In 1969, there were over 55,000 people killed on
the nation's highways and another 2,000,000 seri­
ously injured. The cost of these accidents esti­
imated by the National Safety Council exceeds 11.3
billion dollars.

The number of railroad train derailments has in­
creased over 100 percent in the last five years.
There were 5,487 in 1968 alone, and the rate is
going up.

There were 1,500 fatalities at railroad crossings
in 1968.

In 1969, there were 27 occasions where railroad
accidents required the evacuation of populated
areas due to the hazardous cargo involved.
Twenty-five of the accidents were considered to
be major and resulted in explosion, fire, or
lethal contamination of the surrounding area.

The shipment of hazardous cargo (poisons - pesti­
cides - explosives - flammables, etc.) by rail,
truck, and air is regulated by a tariff written
and controlled by a non-government agency.

With these, and other facts identified, the need
for the application of aerospace techniques to
the solution of the problems became obvious.

Hopefully this paper will generate an interest by
the civic community for the application of proven
techniques to the resolution of civic problems
which exist today. The discussion of the techni­
que is descriptive rather than specific for rea­
sions of brevity. However, there are many who are
familiar with the techniques and agree the ap­
proach has merit.

THEORY OF APPLICATION
For many years the aerospace industry has used
scientific analytical techniques for assuring
system safety and reliability. Typical of these
techniques are:

Preliminary Hazard Analysis
Operations Safety Analysis
Human Error Prediction
Logic Diagram Analysis

These techniques were widely used to assure the
safety and reliability of systems such as Minuteman and Saturn/Apollo. The importance of positive
system assurance within these programs is obvious.
In the case of Minuteman, failure could be cata­
strophic and in the case of Saturn/Apollo, loss of
the astronaut crew, not to mention the tremendous
loss in terms of dollars and national prestige.

The development and application of such analyses
did not occur overnight. It was a long and some­
time painful road for the developers and advocates
of the techniques. Like many new developments,
the advocates are frequently considered to be
"cultists" for which the program is better off
without, or at best, are only to be tolerated.

As the techniques were improved and their value to
the program demonstrated, the discipline of relia­
bility and system safety engineering was gradually
accepted and is now a mandatory requirement in all
major DOD- and NASA- sponsored programs.

The logic diagram, sometimes called fault tree, is
a deductive analytical technique which lends it­
self to detailed system analysis, decision-logic,
and communication. It results in a graphic and
logical representation of the various combinations
of possible events, occurring within a system,
which can cause a predefined undesired event.

An undesired event is any event which is identi­
ﬁed as objectionable or unwanted, such as a po­
tential accident, hazardous condition, or undesired
rate increase. (Correlated to the civic applica­
tion, the undesired event might be fatality at a
railroad crossing, insufficient controls for ship­
ment of hazardous cargo, or increased accident
rate.)
During the development phase of a major program such as Minuteman, emphasis is devoted to the assurance that undesirable events will not occur to the operational system. To provide this assurance each theoretical undesired event is assumed. The logic tree is then developed to determine what event or series of events could cause the undesirable event. For example, if the assumed undesired event was accidental rocket engine ignition, the causative event could be inadvertent closure of relay contacts.

In applying the logic diagram technique to a civic problem, a major change to the aerospace technique is necessary. Whereas, in the above example, we assume certain undesirable events and then determine what can cause them, in the civic application the undesirable condition now exists and we determine the cause. A subtle, but important difference.

Figure 1 is a modified version of the logic diagram of a specific problem of the civilian community. This condition is selected because it allows for a mental exercise of the logic diagram application. Those who are familiar with the technique will notice two major departures from the accepted practice of constructing the diagrams:

1. The absence of AND gates - OR gates.
2. The top undesired event is an existing condition and the segments are results of the condition. Whereas, classically, the top event would be the undesired event and the segments the causative events.

DEVELOPING THE LOGIC DIAGRAM

Figure 1 diagrams the results of INSUFFICIENT URBAN MASS TRANSPORTATION. The diagram depicts two prime branches.

1. INCREASED USE OF INTERNAL COMBUSTION ENGINES
2. GHETTO GROWTH

The populace which must work in the metropolitan area are faced with two choices: either move into the city or drive to and from employment from an urban area. Moving into the city is not necessarily considered an undesirable result of insufficient urban mass transportation; however, it does contribute to the growth of ghetto areas when there is an ethnic attraction. The use of internal combustion engines is undesirable because of the pollution increase.

Following the ghetto growth branch of the diagram we identify many undesirable results such as CRIME INCREASE, WELFARE DEMAND INCREASE, EDUCATIONAL FACILITY DEMANDS, AND ESTHETIC POLLUTION INCREASE. Each of these undesirable conditions resulting from ghetto growth would be diagrammed in detail. Other undesirable results would be identified and diagrammed in detail; e.g., riot and demonstration potential. For purposes of this paper, the diagram has been simplified to demonstrate the application of the technique.

Following the diagram through the ESTHETIC POLLUTION INCREASE branch, we can identify the INCREASED USE OF OLD AUTOMOBILES which in turn leads to the INABILITY TO MAINTAIN SAFETY STANDARDS and/or STEALS TO MAINTAIN SAFETY STANDARDS. These undesirable conditions lead directly to INCREASED ACCIDENT RATE, FAMILY ADDED TO WELFARE ROL直径 INCREASED CRIME RATE. Similar logic is used in defining the branch under INCREASED USE OF INTERNAL COMBUSTION ENGINES.

After the diagram has been completed, a valid assessment of INSUFFICIENT URBAN MASS TRANSPORTATION can be made. Qualitative assessment of this particular logic diagram, as simple as it is, shows graphically that INSUFFICIENT URBAN MASS TRANSPORTATION causes or contributes to:

- Ghetto Growth
- Increased Pollution
- Increased Crime
- Increased Accident
- Degradation of Metropolitan Area
- Increased Welfare Requirements

These conditions require expenditure of tax dollars. The expenditure becomes an ever increasing tax burden which might more profitably be expended in the reduction or elimination of the cause rather than reacting to the results of the condition.

Many of the undesired results, due to INSUFFICIENT URBAN MASS TRANSPORTATION, should be analyzed by separate logic diagrams. For example: INCREASED ACCIDENT RATE which shows up in both branches of the logic tree would be treated as a separate diagram. For purposes of depicting the scope of the analytical technique, one result of increased accident rate is aggravation of serious injury following accident (Figure 2). This event and each of the causes which aggravate the injury, is identified and possible solutions of the cause proposed. This logic technique performed by experienced analysts portrays the complete picture and allows responsible officials to initiate corrective measures. Frequently the determination of increasing the urban transportation media is based on the financial success of the media amortized by the fares received over a period of time. However, if the true costs of insufficient transportation is assessed considering the costs of pollution, crime, accidents, welfare, etc., it might very well be more cost effective to the community to subsidize the media.

The previous discussion concerned an extremely broad and complex problem which exists in many metropolitan areas. The condition was selected so that the potential of the logic diagram analysis could be demonstrated.
CONTROL OF HAZARDOUS CARGO TRANSPORTATION

A more specific application is shown in Figure 3. This problem, INADEQUATE CONTROL OF HAZARDOUS CARGO TRANSPORTATION, is "real world" and should receive priority attention throughout the country. In 1969, there were 25 major railroad accidents involving hazardous materials. Major in this instance includes: fire, explosion, contamination, and evacuation of populace. Each occurred in sparsely populated areas. Figure 4 describes three which are typical. There were hundreds of cases where hazardous cargo, such as Class B poisons, leaked during truck or rail transport. Thousands of cases are suspected.

The logic tree (Figure 3) is constructed as previously described. The existing undesirable condition is shown as the top segment of the tree. (In this instance, the diagram analyzes only poisons (pesticides, etc.)). The subsequent branches of the tree are results of the top undesirable condition. For the sake of brevity, the logic involved in the preparation of the tree will not be discussed. Suffice to say that each branch and segment of the tree represents a condition which did occur during 1969 and was the result of inadequate controls. Each of the segments of this tree would be represented in a separate diagram to describe the specific event. For example: CONTAINER NOT ADEQUATE FOR CONTENT is a prime candidate based on the number of leaks discovered in 1969.

After the problems associated with INADEQUATE CONTROL OF HAZARDOUS CARGO TRANSPORTATION are defined in the logic diagram, there is a need to develop preventive measures. The use of the Preliminary Hazard Analysis technique provides a method for satisfying that need. (Figure 5).

Figure 5 is a Preliminary Hazard Analysis which the analyst develops based on the information he derives from the logic diagram. This analysis describes the hazardous condition in brief terms and provides the accident prevention measures necessary for its control. As a result of this analysis, new or more stringent standards, different inspection methods, additional training, etc., are developed and implemented.

A third application of the logic diagram technique is shown in Figure 6, LACK OF A BALANCED AND INTEGRATED SAFETY PLAN. Unless the state generates an integrated safety plan which defines in detail the role of all agencies responsible for safety, the results will be as shown on the diagram. The capability to efficiently react to a catastrophic condition does not exist nor is preventive safety given the emphasis it deserves. The tax dollar expended for safety is generally wasted for the results achieved. When results of the undesired event are diagramed in this fashion, a rational prioritization of effort and funds can be made to optimize the safety of the community.
**SOLUTION CONSIDERATIONS**

- Use of helicopter ambulance
- Provide directional traffic indicators to direct traffic to single lane - traffic indicators controlled from central station
- Provide emergency traffic lane in future main arterial highways. This lane not to be used for regular traffic.
- Provide emergency vehicles at locations that have a history of high accident rates during predictable hours of occurrence
- Provide emergency telephones at intersections where communications for help would be difficult

- Provide training of ambulance & rescue personnel in emergency response techniques
- Establish state controlled rescue & emergency safety schools
- Provide ambulance & rescue vehicles with modern anti-flammability rescue equipment similar to New York Port Authority
- Utilize experience of nonflammable materials research such as that developed in the Apollo Program
- Work with NBS to make standard for future auto manufacture
- Work with NBS to require rupture proof bag tanks & self-extinguishing fire systems on future auto manufacture

**SOLUTION CONSIDERATIONS**

- Traverse or rough terrain
- Vehicle or hand carry not possible
- Provide directional traffic indicators to direct traffic to single lane
- Provide emergency telephones on highways where communications for help would be difficult

- Training of emergency crew (ambulance - police) at schools similar to Army Rangers
- Use of helicopter
- Rescue equipment included in rescue equipment

**SOLUTION CONSIDERATIONS**

- Late arrival of medical aid
- Inadequate training
- Non-availability of proper tools
- Fire or structural damage
- Inadequate telephone
- Travelling through or rough terrain
- Vehicle or hand carry not possible
- Provide directional traffic indicators to direct traffic to single lane
- Provide emergency telephones on highways where communications for help would be difficult

- Same solution considerations as late arrival of medical aid
- Provide rescuer vehicle maintenance is not neglected
- Provide stringent drivers test for emergency vehicle drivers
- Provide special high speed defensive driving course
- Design vehicle for maximum emergency absorption during impact
- Ensure restraints for cargo such as litters, rescue tools, etc. to prevent movement during impact
- Provide inflatable bag concept for attendants and the injured

*Figure 2*
# ACCIDENTS INVOLVING HAZARDOUS MATERIALS

<table>
<thead>
<tr>
<th>EVENT</th>
<th>CAUSE</th>
<th>HAZARDOUS MATERIAL</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>- TRAIN DERAILED</td>
<td>- WHEEL BROKE</td>
<td>- PROPANE GAS</td>
<td>- 14 CARS DERAILED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- RAILROAD CAR EXPLOSION</td>
<td>- HOT BOX - FIRE - MOVING TRAIN</td>
<td>- 750 LB BOMBS - REMOTE LOCATION</td>
<td>- 4 CRATERS 20' WIDE X 50' LONG</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- RAILROAD TRAIN DERAILED &amp; COLLISION</td>
<td>- BROKEN RAIL WHICH WAS FORGED IN 1929</td>
<td>- CYANIDE</td>
<td>- TOWN OF 250 EVACUATED FOR 2 DAYS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4
### Preliminary Hazard Analysis

<table>
<thead>
<tr>
<th>System or Function</th>
<th>Mode</th>
<th>Hazardous Element</th>
<th>Event Causing Hazardous Condition</th>
<th>Hazardous Condition</th>
<th>Event Causing Potential Accident</th>
<th>Potential Accident</th>
<th>Effect and Hazard Class</th>
<th>Accident Prevention Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tanker or Carrier Truck</td>
<td>Maneuvering</td>
<td>Class &quot;B&quot; Flammable Liquid</td>
<td>Spill/Leakage, Hauling, Wildfire Travel</td>
<td>Leakage</td>
<td>Spontaneous Combustion</td>
<td>Fire Explosion</td>
<td>I: Death or Injury to Personnel and Animals</td>
<td>Conform to OSHA Regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PerIOD蒋 INSPECTION TO STATE STANDARDS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PERIODIC HYDROSTATIC TEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>GENERATE STANDARDS FOR CHARGING OF SOFTWARE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DEVELOP EMERGENCY PRODUCTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DEVELOP HAZARDOUS ELEMENTS DETECTION</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DEVELOP CONTAMINATION PROCEDURES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ESTABLISH DECONTAMINATION PROCEDURES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ESTABLISH INTERFACE PROCEDURES WITH NATIONAL DEF HAZARDOUS CARGO COMMITTEE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PROVIDE BI-LATERN COMMUNICATION NET</td>
</tr>
</tbody>
</table>

**Figure 5**
Figure 6

Diagram showing the lack of balanced and integrated safety plan due to various issues:

- Many incidents on record
- Inability to efficiently react to disaster or catastrophe
- Disaster control plan not developed
- Coordination of all concerned agencies not established
- Disaster control plan difficult to implement
- Life and property losses increase
- Limited and non-coordinated state safety
- Safety responsibility assigned to various agencies
- Nonenforcement of federal and state standards
- Public confusion
- Increased accident rate
- Flow of safety data to different agencies
- State subject to different agencies
- State subject to legal scrutiny
- Emphasis directed to immediate problems
- Safety emphasis in areas of local knowledge only
- Proven safety practices not used
- Preventive safety degraded