The Space Congress® Proceedings

1971 (8th) Vol. 1 Technology Today And Tomorrow

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

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 continue 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 application of reliability and system safety analytical 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 seriously injured. The cost of these accidents estimated by the National Safety Council exceeds 11.3 billion dollars.

The number of railroad train derailments has increased 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 - pesticides - 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 technique is descriptive rather than specific for reasons of brevity. However, there are many who are familiar with the techniques and agree the approach 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 catastrophic 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 sometime 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 reliability 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 itself 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 identified as objectionable or unwanted, such as a potential accident, hazardous condition, or undesired rate increase. (Correlated to the civic application, the undesired event might be fatality at a railroad crossing, insufficient controls for shipment 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 undesired conditions lead directly to INCREASED ACCIDENT RATE, FAMILY ADDED TO WELFARE ROLES and 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 sparsly 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.

ILLUSTRATIONS

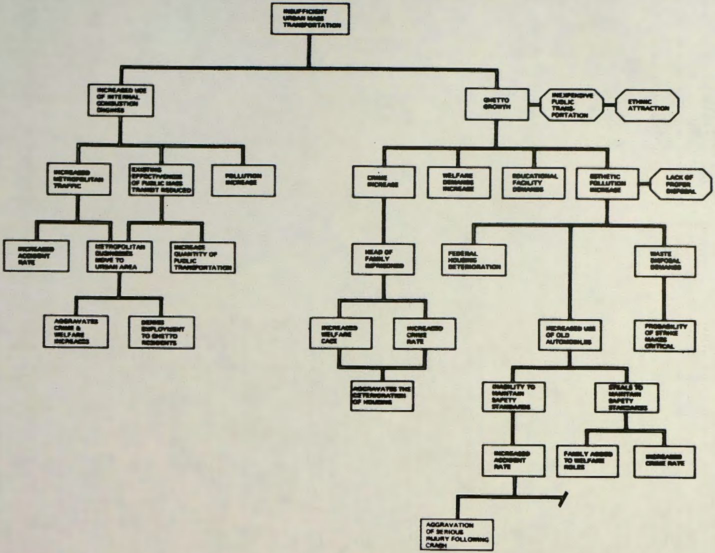
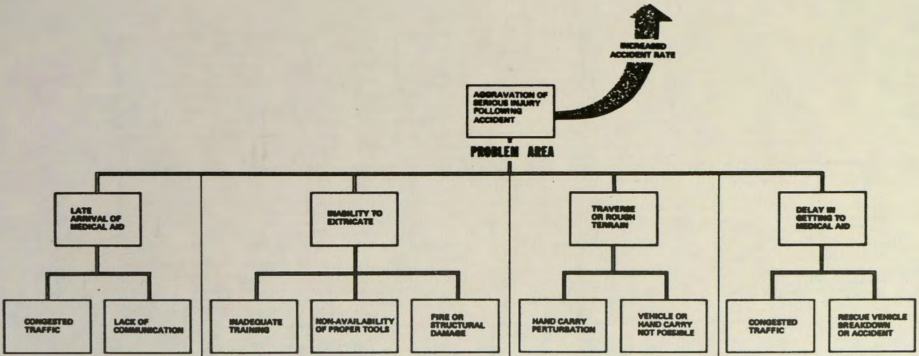

INSUFFICIENT URBAN MASS TRANSPORTATION
INCREASED USE OF INTERNAL COMBUSTION ENGINES
GHETTO GROWTH
INEXPENSIVE PUBLIC TRANS-PORTATION
ETHNIC ATTRACTION
INCREASED METROPOLITAN TRAFFIC
EXISTING EFFECTIVENESS OF PUBLIC MASS TRANSIT REDUCED
POLLUTION INCREASE
CRIME INCREASE
WELFARE DEMANDS INCREASE
EDUCATIONAL FACILITY DEMANDS
ESTHETIC POLLUTION INCREASE
LACK OF PROPER DISPOSAL
INCREASED ACCIDENT RATE
METROPOLITAN BUSINESSES MOVE TO URBAN AREA
INCREASE QUANTITY OF PUBLIC TRANSPORTATION
HEAD OF FAMILY IMPRISONED
FEDERAL HOUSING DETERIORATION
WASTE DISPOSAL DEMANDS
AGGRAVATES CRIME & WELFARE INCREASES
DENIES EMPLOYMENT TO GHETTO RESIDENTS
INCREASED WELFARE CASE
INCREASED CRIME RATE
INCREASED USE OF OLD AUTOMOBILES
PROBABILITY OF STRIKE MAKES CRITICAL
AGGRAVATES THE DETERIORATION OF HOUSING
INABILITY TO MAINTAIN SAFETY STANDARDS
INCREASED ACCIDENT RATE
FAMILY ADDED TO WELFARE ROLES
INCREASED CRIME RATE
AGGRAVATION OF SERIOUS INJURY FOLLOWING CRASH

Figure 1



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 ON HIGHWAYS WHERE COMMUNICATIONS FOR HELP WOULD BE DIFFICULT

SOLUTION CONSIDERATIONS

- PROVIDE TRAINING OF AMBULANCE & RESCUE PERSONNEL IN EGRESS/INGRESS TECHNIQUES
- ESTABLISH STATE CONTROLLED RESCUE & EMERGENCY SAFETY SCHOOLS
- PROVIDE AMBULANCE & RESCUE VEHICLES WITH MODERN INGRESS RESCUE EQUIPMENT – SIMILAR TO NEW YORK PORT AUTHORITY
- UTILIZE EXPERIENCE OF NONFLAMMABLE MATERIAL RESEARCH SUCH AS THAT DEVELOPED IN THE APOLLO PROGRAM
  - WORK WITH NHSB TO MAKE STANDARD FOR FUTURE AUTO MANUFACTURE
  - WORK WITH NHSB TO REQUIRE RUPTURE PROOF GAS TANKS & SELF EXTINGUISHING FIRE SYSTEMS ON FUTURE AUTO MANUFACTURE

SOLUTION CONSIDERATIONS

- TRAINING OF EMERGENCY CREW (AMBULANCE – POLICE) AT SCHOOLS SIMILAR TO ARMY RANGERS
- USE OF HELICOPTER
- RIGGING EQUIPMENT INCLUDED IN RESCUE EQUIPMENT

SOLUTION CONSIDERATIONS

- SAME SOLUTION CONSIDERATIONS AS LATE ARRIVAL OF MEDICAL AID
- ASSURE RESCUE VEHICLE MAINTENANCE IS NOT NEGLECTED
- PROVIDE STRINGENT DRIVERS TEST FOR EMERGENCY VEHICLE DRIVERS
- PROVIDE SPECIAL HIGH SPEED DEFENSIVE DRIVING COURSE
- DESIGN VEHICLE FOR MAXIMUM ENERGY 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

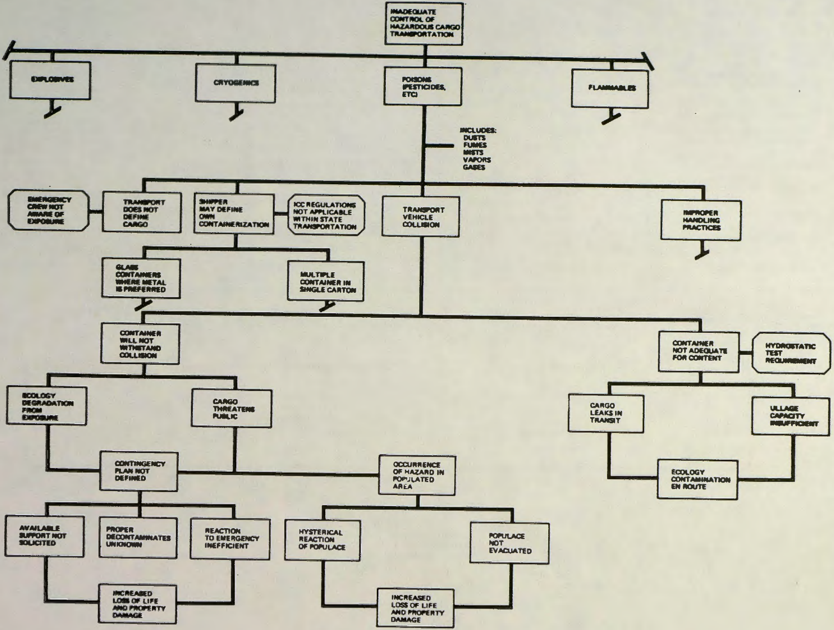

INADEQUATE CONTROL OF HAZARDOUS CARGO TRANSPORTATION
EXPLOSIVES
CRYOGENICS
POISONS (PESTICIDES, ETC)
FLAMMABLES
INCLUDES: DUSTS FUMES MISTS VAPORS GASES
EMERGENCY CREW NOT AWARE OF EXPOSURE
TRANSPORT DOES NOT DEFINE CARGO
SHIPPER MAY DEFINE OWN CONTAINERIZATION
ICC REGULATIONS NOT APPLICABLE WITHIN STATE TRANSPORTATION
TRANSPORT VEHICLE COLLISION
IMPROPER HANDLING PRACTICES
GLASS CONTAINERS WHERE METAL IS PREFERRED
MULTIPLE CONTAINER IN SINGLE CARTON
CONTAINER WILL NOT WITHSTAND COLLISION
CONTAINER NOT ADEQUATE FOR CONTENT
HYDROSTATIC TEST REQUIREMENT
ECOLOGY DEGRADATION FROM EXPOSURE
CARGO THREATENS PUBLIC
CARGO LEAKS IN TRANSIT
ULLAGE CAPACITY INSUFFICIENT
CONTINGENCY PLAN NOT DEFINED
OCCURRENCE OF HAZARD IN POPULATED AREA
ECOLOGY CONTAMINATION EN ROUTE
AVAILABLE SUPPORT NOT SOLICITED
PROPER DECONTAMINATES UNKNOWN
REACTION TO EMERGENCY INEFFICIENT
HYSTERICAL REACTION OF POPULACE
POPULACE NOT EVACUATED
INCREASED LOSS OF LIFE AND PROPERTY DAMAGE
INCREASED LOSS OF LIFE AND PROPERTY DAMAGE

Figure 3

ACCIDENTS INVOLVING HAZARDOUS MATERIALS

EVENT	- TRAIN DERAILMENT - LAUREL, MISSISSIPPI, JANUARY 25, 1969
CAUSE	- WHEEL BROKE
HAZARDOUS MATERIAL	- PROPANE GAS
RESULT	- 14 CARS DERAILED 2 FATALITIES 33 HOSPITALIZED 60 HOMES DESTROYED EVACUATION OF 1000 POPULACE BURNING MATERIEL/FRAGMENTS SCATTERED 1/2 MILE RADIUS

EVENT	- RAILROAD CAR EXPLOSION - WELLS, NEVADA, JULY, 1969
CAUSE	- HOT BOX - FIRE - MOVING TRAIN
HAZARDOUS MATERIAL	- 750 LB BOMBS - REMOTE LOCATION
RESULT	- 4 CRATERS 20' WIDE X 50' LONG FRAGMENTATION UP TO 1/2 MILE

EVENT	- RAILROAD TRAIN DERAILMENT & COLLISION -DUNRIETH, INDIANA, JANUARY 1968
CAUSE	- BROKEN RAIL WHICH WAS FORGED IN 1929
HAZARDOUS MATERIAL	- CYANIDE
RESULT	- TOWN OF 250 EVACUATED FOR 2 DAYS COLLISION WITH FREIGHT TRAIN OF 106 CARS APPROXIMATELY 200 BUSINESSES & HOMES DESTROYED/DAMAGED CYANIDE POLLUTION OF LOCAL WATER - SEVERAL MONTHS

Figure 4

PRELIMINARY HAZARD ANALYSIS

SYSTEM OR FUNCTION	MODE	HAZARDOUS ELEMENT	EVENT CAUSING HAZARDOUS CONDITION	HAZARDOUS CONDITION	EVENT CAUSING POTENTIAL ACCIDENT	POTENTIAL ACCIDENT	EFFECT AND HAZARD CLASS	ACCIDENT PREVENTION MEASURES		
								HARDWARE	PROCEDURES	PERSONNEL
TANKER OR CARGO TRUCK	HANDLING STORAGE LOADING UNLOADING TRAVEL	CLASS "B" POISON (DUST - SOLIDS - MISTS - VAPORS LIQUIDS) i.e., ARSENICS BARIUM CYANIDE CLOROPICRIN COMPOUNDS TREE OR WEED KILLING CYANIDES DINITROPHENOLS, ETC.	LEAKAGE SPILLAGE RUPTURE	ENVIRONMENT IS EXPOSED TO POISON DUST - MISTS - VAPORS OR LIQUIDS	SPONTANEOUS COMBUSTION AUTO IGNITION HYPERGOLIC REACTION SPARK OR FLAME HIGHWAY ACCIDENT	TOXICITY FIRE EXPLOSION AREA OF CONTAMINATION EXPANDED BY POISONOUS LIQUID OR DUST ENTERING RIVERS, STREAMS OR SEWAGE POISON VAPORS AND DUST CARRIED BY WIND	I DEATH OR INJURY TO PERSONNEL AND ANIMALS II SEVERE ECOLOGY DAMAGE I LONG TERM RESIDUAL DANGER I PERSONNEL EXPOSURE TO CONTAMINATED PRODUCE	CONFORM TO ICC REGULATIONS PERIODIC INSPECTION TO STATE STANDARDS PERIODIC HYDROSTATIC TEST GENERATE STANDARD FOR CHANGEOUT OF SOFTWARE TANK OR SHIPPING CONTAINER DESIGN APPROVAL BY STATE SAFETY DIRECTOR ICC REGULATION PART 78 PROVIDE IN-TRANSIT COMMUNICATION NET	ESTABLISH HANDLING, STORAGE, LOADING AND OFF-LOADING PROCEDURES DEVELOP EMERGENCY PROCEDURES DEVELOP HAZARDOUS ELEMENTS DETECTION DEVICES/SYSTEMS ESTABLISH DECONTAMINATION PROCEDURES ESTABLISH INTERFACE PROCEDURES WITH NATIONAL DOT HAZARDOUS CARGO COMMITTEE	PROVIDED PROTECTIVE CLOTHING & BREATHING APPARATUS FOR DRIVERS MEDICAL CERTIFICATION PROGRAM CLASS "B" POISON TRAINING PROGRAM INCLUDE: HIGHWAY PATROL FIRE DEPARTMENT LOCAL POLICE CIVIL DEFENSE
		EXPLOSIVES	EXCESSIVE TEMPERATURE LEAKAGE EXPOSURE TO IGNITION SOURCE	PUBLIC AND PROPERTY EXPOSED TO EXPLOSION AND FRAGMENTATION	FIRE IMPACT SHOCK ELECTRICAL MECHANICAL SPARK	EXPLOSION FRAGMENTATION SYMPATHETIC DETONATION				
		FLAMMABLES	LEAKAGE SPILLAGE RUPTURE EXPOSURE TO IGNITION SOURCE	PUBLIC AND PROPERTY EXPOSED TO FIRE	FIRE SPARK STATIC ELECTRICITY AUTO IGNITION SPONTANEOUS COMBUSTION VAPOR IGNITION					
		CRYOGENICS	LEAKAGE RUPTURE SPILLAGE PRESSURE BUILDING	PUBLIC AND PROPERTY EXPOSED TO SEVERE COLD, EXPLOSION AND FIRE	BOIL-OFF FAILURE IMPACT SHOCK REACTION WITH OTHER CRYOGENICS FIRE	TOXICITY FIRE EXPLOSION DEWAR				

SAMPLE

Figure 5

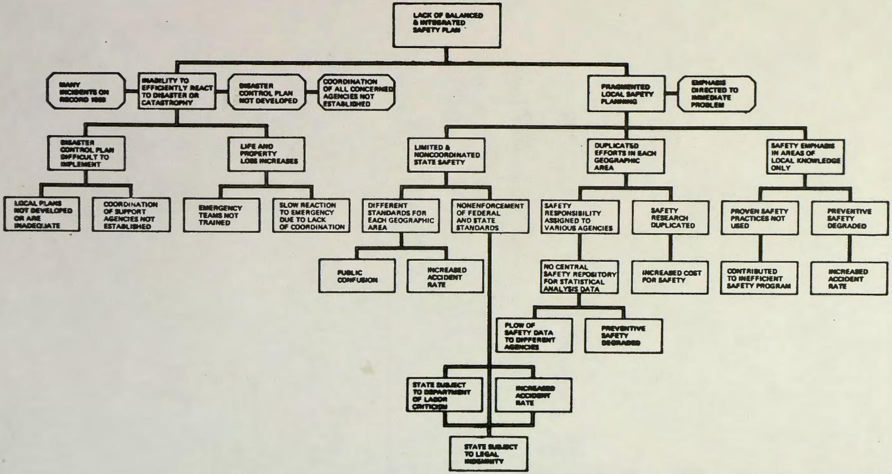

LACK OF BALANCED & INTEGRATED SAFETY PLAN
MANY INCIDENTS ON RECORD
INABILITY TO EFFICIENTLY REACT TO DISASTER OR CATASTROPHY
DISASTER CONTROL PLAN NOT DEVELOPED
COORDINATION OF ALL CONCERNED AGENCIES NOT ESTABLISHED
FRAGMENTED LOCAL SAFETY PLANNING
EMPHASIS DIRECTED TO IMMEDIATE PROBLEM
DISASTER CONTROL PLAN DIFFICULT TO IMPLEMENT
LIFE AND PROPERTY LOSS INCREASES
LIMITED & NONCOORDINATED STATE SAFETY
DUPLICATED EFFORTS IN EACH GEOGRAPHIC AREA
SAFETY EMPHASIS IN AREAS OF LOCAL KNOWLEDGE ONLY
LOCAL PLANS NOT DEVELOPED OR ARE INADEQUATE
COORDINATION OF SUPPORT AGENCIES NOT ESTABLISHED
EMERGENCY TEAMS NOT TRAINED
SLOW REACTION TO EMERGENCY DUE TO LACK OF COORDINATION
DIFFERENT STANDARDS FOR EACH GEOGRAPHIC AREA
NONENFORCEMENT OF FEDERAL AND STATE STANDARDS
SAFETY RESPONSIBILITY ASSIGNED TO VARIOUS AGENCIES
SAFETY RESEARCH DUPLICATED
PROVEN SAFETY PRACTICES NOT USED
PREVENTIVE SAFETY DEGRADED
PUBLIC CONFUSION
INCREASED ACCIDENT RATE
NO CENTRAL SAFETY REPOSITORY FOR STATISTICAL ANALYSIS DATA
INCREASED COST FOR SAFETY
CONTRIBUTED TO INEFFICIENT SAFETY PROGRAM
INCREASED ACCIDENT RATE
FLOW OF SAFETY DATA TO DIFFERENT AGENCIES
PREVENTIVE SAFETY DEGRADED
STATE SUBJECT TO DEPARTMENT OF LABOR CRITICISM
INCREASED ACCIDENT RATE
STATE SUBJECT TO LEGAL INDEMNITY

Figure 6