AD-A046 288 BATTELLE COLUMBUS LABS OHIO F/G 13/10
SYSTEM SAFETY ANALYSIS OF A COMMERCIAL VESSEL.(U)
NOV 77 E S CHEANEY, A J COYLE DOT-CG-42087-A
UNCLASSIFIED BATT-G-2955-0001 USCG-D-39-77 NL

1 OF 2
AD
A046288



Report No. CG-D-39-77

AD A046288

SYSTEM SAFETY ANALYSIS OF A COMMERCIAL VESSEL

FINAL REPORT

NOVEMBER 1977

DDC RECEIVED NOV 9 1977 A

Document is available to the public through the National Technical Information Service, Springfield, Virginia 22151

AD No. DDC FILE COPY

Prepared for

DEPARTMENT OF TRANSPORTATION
UNITED STATES COAST GUARD
Office of Research and Development
Washington, D.C. 20590

NOTICE

This document is disseminated under the sponsorship of The U. S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The work reported herein was performed for the United States Coast Guard Office of Research and Development, Marine Safety Technology Division, as part of its program in Commercial Vessel Safety for the Office of Merchant Marine Safety. This work is being performed by Battelle's Columbus Laboratories under Contract Number DOT-CG-42087-A.

Technical Report Documentation Page

1. Report No. (18) USCG-D-39-77 (19)	2. Government Accession No.	3. Recipient's Catalog No. (11) Nov 77
4. Title and Subtitle (6) SYSTEM SAFETY ANALYSIS OF A COMMERCIAL VESSEL.		5. Report Date November 1977
		6. Performing Organization Code (12) 127p.
7. Author(s) (10) E. S. Cheaney and A. J. Coyle		8. Performing Organization Report No. (14) BATT G-2955-0001
9. Performing Organization Name and Address BATTELLE COLUMBUS LABORATORIES 505 King Avenue Columbus, Ohio 43201		10. Work Unit No. (TRAIS)
		11. Contract or Grant No. (15) DOT-CG-42087-A
12. Sponsoring Agency Name and Address DEPARTMENT OF TRANSPORTATION United States Coast Guard Office of Research and Development 400 Seventh Street, S.W., Washington, D.C. 20590		13. Type of Report and Period Covered (9) Final Task Report.
		14. Sponsoring Agency Code G-DST

15. Supplementary Notes

The United States Coast Guard Research and Development's Technical Representative for the work performed herein was D. E. Laaksonen.

16. Abstract

This report describes a limited system safety analysis carried out on a commercial vessel. The purpose of conducting the study was to (1) develop a set of inspection criteria derived from a system safety study, (2) demonstrate the application of system safety analysis methodology to a commercial vessel, and (3) identify/define needed modifications to VIIS as currently being developed for the Coast Guard. The safety analysis was limited to a study of fire/explosion hazards in the vessel's cargo/cargo transfer system. The vessel studied was a 38,000 ton special products carrier hauling gasoline, other petrochemicals, and industrial chemicals in a cargo system consisting of 27 tanks and 21 pumps.

Three types of analyses were conducted: preliminary hazards, logic diagram, and hazard mode and effect. Findings were based on study documentation and plans for the vessel plus two on-board inspections, one of which included a six-day voyage. The commercial vessel environment proved entirely amenable to system safety analysis procedures. Although no unexpected or unusual hazards were identified, it was found feasible and reasonable to construct a safety critical profile for the vessel. The impact on the design of VIIS was judged to be minor and well within planned capabilities.

17. Key Words	18. Distribution Statement		
Commercial Vessel System Safety Merchant Marine Safety Vessel Inspection	DISTRIBUTION STATEMENT A Approved for public release; Distribution Unlimited		
19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified		

Form DOT F 1700.7 (8-72)

407080

TABLE OF CONTENTS

		Page
1.0	INTRODUCTION	1
	1.1 BACKGROUND	1
2.0	PROCEDURE	3
	2.1 VESSEL SELECTION	3
	2.2 FAMILIARIZATION AND PRELIMINARY HAZARDS STUDY	6
	2.3 ONBOARD SAFETY STUDY	7
	2.4 ANALYSIS AND REPORTING	8
3.0	RESULTS	8
	3.1 INSPECTION CRITERIA--AN EXAMPLE SCP	9
	3.2 INSPECTION RELATED DATA	9
	3.3 APPLICABILITY OF THE ANALYSIS TECHNIQUES TO COMMERCIAL VESSELS	12
	3.4 CRITERIA FOR CRITICALITY	15
	3.5 UTILITY OF THIS STUDY AS A DEMONSTRATION	16
4.0	SYSTEM SAFETY ANALYSIS	18
	4.1 THE COMMERCIAL VESSEL ACCIDENT ENVIRONMENT	19
	4.1.1 *Party-at-Risk Categories*	20
	4.1.2 Accident Type Categories	22
	4.2 PRELIMINARY HAZARDS ANALYSIS	23
	4.2.1 PHA Technique	24
	4.2.2 Study Vessel PHA	27
	4.2.3 Selection of Scope for More Detailed Safety Analyses	31
	4.3 LOGIC DIAGRAM ANALYSIS	31
	4.3.1 Pump Room Fires and Explosion Study	33
	4.3.2 Cargo Tank Fires and Explosions Study	39
	4.3.3 Topside Area Fire and Explosion Study	47
	4.3.4 Fire and Explosion Hazard Analysis	49
	4.4 HAZARD MODE AND EFFECT ANALYSIS	64
	4.4.1 Components and Subsystems Analyzed	64
	4.4.2 Development of the HMEA Format	66
	4.4.3 Conduct of the HMEA	69

TABLE OF CONTENTS
(Continued)

Page

4.5 CRITIQUE OF ANALYSIS TECHNIQUES 73

4.5.1 Tractability of the System Safety Approach 73

4.5.2 Most Useful Techniques 76

4.5.3 Impact of System Safety Analysis on the Design of VIIS 78

4.5.4 Superiority of System Safety Techniques 78

APPENDIX A

STUDY VESSEL DESCRIPTION A-1

APPENDIX B

STUDY VESSEL SYSTEMS B-1

APPENDIX C

SYSTEM SAFETY ANALYSIS RESULTS IMPLEMENTATION PLAN C-1

APPENDIX D

LOGIC DIAGRAM CONSTRUCTION AND SYMBOLOGY D-1

LIST OF TABLES

Table 4-1. Hazard Categories 26

Table 4-2. Criticality Assessment Combinations 55

Table 4-3. Hazard Criticality Assessment 56

LIST OF FIGURES

Figure 3-1. Safety Critical Profile 10

Figure 4-1. Logic Diagram Portraying the Commercial Vessel Accident Environment 21

Figure 4-2. Preliminary Hazards Analysis 28

Figure 4-3. Upper Levels of the Fire and Explosion Diagram 32

Figure 4-4. Event Path D21-E11 Development--"Source of Ignition Present" 35

LIST OF FIGURES
(Continued)

Page

Figure 4-5. Event Path E12 Development--"Explosive Mixture Present". 37

Figure 4-6. Event E13 Development--"Foam System Not Effective" . . . 40

Figure 4-7. Event Path D22-E21 Development--"Cargo Tank Fire A/O Explosion During Cargo Transfer" 42

Figure 4-8. Event Path E22 Development--"Cargo Tank Fire and/or Explosion During Cleaning and Preparation" 45

Figure 4-9. Event Path E23 Development--"Cargo Tank Fire and/or Explosion During Cruising Loaded" 46

Figure 4-10. Event Path E24 Development--"Cargo Tank Fire and/or Explosion During Cruising Unloaded and in Ballast . . . 46

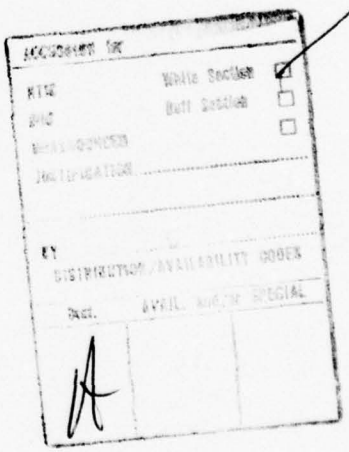
Figure 4-11. Event Path D23 Development--"Fire or Explosion in Topside Area" 48

Figure 4-12. Safety Critical Profile 63

Figure 4-13. Component/Subsystem Listing for HMEA 65

Figure 4-14. Hazard Mode and Effect Analysis 70

Figure 4-15. Safety Critical Profile 74



Preceding Page BLANK - FILMED

SYSTEM SAFETY ANALYSIS OF A COMMERCIAL VESSEL

by

E. S. Cheaney and A. J. Coyle

1.0 INTRODUCTION

As an integral part of its development of the Vessel Inspection Information System (VIIS), Battelle's Columbus Laboratories (BCL) undertook the conduct of a limited system safety analysis of a commercial vessel. The primary purpose of this task was to find out if the use of system safety procedures as a part of the Coast Guard's vessel safety program would in any way affect the design of VIIS so that compatible features could be incorporated in the design if appropriate. Secondary purposes were to explore the potential of system safety procedures for safety assurance in commercial vessels and to provide an example study for future use in the Coast Guard's vessel safety program.

Accordingly, a safety study of the cargo and cargo transfer system of a special products tanker was performed. The study resulted in the construction of a safety critical profile for the system and formulation of a set of criteria and guidelines for the conduct of such studies aboard commercial vessels. This report covers the conduct of the study. Discussions of the study's background, the procedures used, and results achieved follow immediately. The conduct of the safety analysis is described in the subsequent major section. Pertinent information, including a description of the vessel utilized in the study is included in a series of appendices.

1 1 BACKGROUND

The VIIS program is aimed at developing a modern, computerized information system designed to enhance the effectiveness and efficiency with which the Coast Guard performs the vessel inspection function. The system is intended to make a full array of inspection and safety information about a specific vessel immediately available to the inspector in whatever port

the vessel may have an inspection of any kind scheduled or needed. The information will cover the full materiel history of the vessel (including records of all previous inspections), particulars of its design and construction, service history, and special information on safety features and priority inspection items--aspects of the vessel that should be given special attention by the inspector to ensure safe conditions. The latter item of information about a vessel is termed its "safety critical profile" (SCP)*.

The background of this task is rooted in a premise about system safety vis-à-vis the VIIS design which led to the original decision to make the task a part of the VIIS development program. This premise is that such system safety techniques as hazards analysis and risk management comprise a potentially superior way of identifying and analyzing hazards in commercial vessels in advance of the occurrence of accidents and that they will, therefore, be incorporated within the foreseeable future as routine procedures in connection with plan review and certification of new vessels. The results of such activities would, of course, constitute an important set of basic information about a new vessel and should influence decisions about inspection priorities, methods, and procedures connected with the vessel. Obviously, the results of such analyses would become part of VIIS' information content and the system must be designed to have the capability for receiving, manipulating, and retrieving, in useful form, the type of information about a vessel such studies would produce. To do this, the example study was planned to determine the type and best use of such information. At the same time, the example study addressed the broader issues of how such analyses could best be performed and the relative effectiveness of the techniques involved in defining the safety--or lack of it--of a vessel. The task work plan was developed with both the immediate question--how to design VIIS--and these larger issues in mind.

---

* The concept of establishing such profiles for specific vessels or vessel types is new. It was generated in connection with BCL's initial analysis of the kinds of information needed by Coast Guard Inspectors to enhance their effectiveness and efficiency.

1.2 TASK OBJECTIVES

The task was conducted to serve the following three interrelated objectives:

(1) Develop a set of inspection criteria for the experimental vessel (an SCP) derived from conducting a system safety study. In meeting this objective, the task was intended to also accomplish these ends.

- Generate useful inspection data about the study vessel/class
- Measure the power of the system safety methodologies for developing inspection criteria with respect to new vessels or vessel features
- Establish definitions and measures for the parameters governing hazard criticality from the standpoint of the inspection process.

(2) Demonstrate the application of system safety analysis methodology as applied to a major commercial vessel.

(3) Identify and define needed modifications to VIIS.

2.0 PROCEDURE

The procedures used in carrying out the study consisted of four sequential steps: (1) vessel selection, (2) familiarization and Preliminary Hazard Study, (3) onboard safety study, and (4) analysis and reporting.

2.1 VESSEL SELECTION

The study vessel was selected by BCL subject to ratification by the Coast Guard's technical steering committee for this program. A variety of criteria governing the selection appeared over the period of time it was being considered.

The Coast Guard's original RFP specified that the experimental vessel should be a modern, high-speed, cargo vessel. In BCL's proposal, additional selection parameters were suggested:

> "....it is desirable to select a vessel which incorporates features that offer a wide range of potential hazards which could impact the full range of parties at risk. This implies a vessel which carries a wide variety of cargo types and includes a wide variety of subsystems. Also, to facilitate obtaining pertinent vessel data, the vessel design and construction should have been carried out by United States companies and shipyards."

The final selection was based on three additional criteria which evolved as various types of vessels were specifically considered.

> Methodology Challenge. The vessel type should strongly challenge the analysis methodology. To do so, the vessel should not only be of modern design but should reflect some aspect of advancing technology, such as use of advanced materials, handling of new types of hazardous cargoes, or use of advanced means of propulsion or vessel control. Also, the vessel type should incorporate subsystems that are sufficiently complex that hazards will by nonobvious, i.e., their detection requires exercise of rigorous analytical methods and the ability to conceptualize accident chains freely.

> Accident Impact. The vessel type should be such that the potential accidents have the highest impact from the standpoint of the Coast Guard's safety responsibilities. There are two impact elements to be considered: parties-at-risk and environmental risk. A vessel type would be most significant with respect to this criterion if the accidents it is likely to have characteristically threaten (1) severe damage to the general public, as well as the vessel, crew, and cargo; and (2) a spill polluting the marine environment and atmosphere.

> Expected Proportionate Population. The vessel type should be of growing importance in commerce, handling a significant share of the total cargo hauled over water. It should be representative of a substantial part of the foreseeable future population of the types of ships in the merchant fleet--not a one-time-only, highly unique class.

In the search for a vessel meeting these criteria, four types were examined: (1) large tankers which feature the technology of "jumboization", (2) handy-size special-purpose tankers which feature the technology of handling and managing multiple, hazardous cargoes, (3) tankers designed for hauling liquidied natural gas (LNG) which feature the technology of LNG

containment and management, and (4) containerships which feature the technology of container handling and shipboard stowage. All these types offered a good challenge to the safety analysis methodology.

From the standpoint of the kind of hazards most likely to be controllable by inspection as opposed to design, the BCL team concluded that the special-purpose tanker type offered the richest and most productive challenge because of the multiplicity of kinds of hazards present. This conclusion was based on the variety of cargoes handled; their characteristic intrinsic hazardousness, both separately and in combination; and the physical and operational complexity of the cargo-handling systems involved. It was decided that the best choice would be a vessel whose cargo-handling system includes a pump room where several pumps are installed with associated manifolding and valving since this is a recognized high hazard feature of modern tankers. Accidents involving this type of vessel are often collisions or groundings in high traffic areas close to population centers ashore so the general public is threatened by the fires and explosions and toxic release potential of such accidents. Further, this class of vessel is of growing commercial importance as revealed by projected building plans, as well as trends in commodity traffic data.

A suitable vessel of this type was located and the cooperation of her owners was solicited and obtained. By agreement with the owners, she will remain anonymous in this report being referred to simply as the "STUDY VESSEL". She is of 38,000 tons displacement, 660.17' length overall, 90.17' extreme width, and 36.65' summer draft. She has a cargo system consisting of 12 wing tanks and 15 center tanks, totaling a liquid product carrying capacity of 329,000 barrels at 98 percent full. The cargo-handling system consists of 5 centrifugal and 3 reciprocating pumps in an after pump room and 13 deep-well pumps located on the main deck over the tanks they serve. She carries a large variety of petroleum and chemical products on a fixed route between a port on the Gulf Coast and a terminal at a petrochemicals processing complex in the Northeast. The full round trip, including loading and unloading, takes approximately 12 days; the northbound run is loaded while southbound is in ballast. She is steam turbine powered. The general

hull arrangement is conventional with house and propulsion aft. She is 10 years old having been built by Bethlehem Steel at Sparrows Point and put in service in 1966. In the period she has experienced no casualties of significance to this study and has not been modified. A more complete description of the vessel and her systems is given in appendix A. Also included in that appendix is a review of the vessel's history, service, and the specific operating phases comprising her service cycle.

2.2 FAMILIARIZATION AND PRELIMINARY HAZARDS STUDY

After selecting the vessel, the study team was formed consisting of the authors of this report. The following familiarization steps were carried out:

- Coast Guard Documentation. A complete file on microfiche of the Coast Guard's initial documentation concerning the STUDY VESSEL was obtained and studied. This included plans and drawings, specifications, and test schedules and results.

- Owner Familiarization. The owner's main offices were visited to interview key individuals concerned with the safety and operation of the vessel and to study the documents and files concerning the vessel maintained by the home office.

- Vessel Familiarization Visit. The study team visited the vessel for a day while she was unloading at the northern terminal. A general inspection of the ship was carried out; interviews were held with the Chief Mate and Chief Engineer; and arrangements were finalized for the team's subsequent cruise aboard the vessel to do the safety job.

During and immediately following these familiarization steps, the team carried out a preliminary hazards analysis of the STUDY VESSEL. Its purposes were to list the main hazards in the vessel in her various operational phases and to order these into a top-level accident environment. In connection with this study, the vessel's main systems and their involvement in the different accident categories were defined and described. Appendix B of this report gives the main system breakdown used.

Based on this study, preliminary decisions were made as to which of the vessel's systems would be studied in detail and which category of accidents would be used in making the detailed study. At this point, it was

decided to concentrate the safety analysis on accidents involving fires or explosions in the cargo and cargo-transfer system. The decision was based on the technical complexity of the system and phenomena involved which seemed to offer the best corpus on which to try the system safety analysis techniques and on the current criticality of this class of accidents to the Coast Guard's vessel safety program.

2.3 ONBOARD SAFETY STUDY

The study team boarded the vessel shortly after it arrived at its northern terminal and began the unloading process; they observed the unloading and then rode the vessel on its southbound voyage leaving shortly after the ship tied up and began the job of loading cargo. During the voyage, the team observed in detail all the operations concerned with the cargo system, i.e., ballasting, washing down empty tanks, handling cleaning slops, gas-freeing, cleaning tanks, and conducting a number of other cargo system maintenance operations (including a major job of renewing the expansion joints in most of the main deck cargo piping). The onboard cargo system administration/accountability setup was examined in detail with special reference to safety responsibilities and their manner of discharge. Informal discussions, many in considerable depth, were held with officers and crewmen concerning a variety of safety matters and past experiences. The attitude and cooperativeness of all the people aboard the STUDY VESSEL were outstandingly good--they took a real interest in the study and its purposes and were anxious to be of help.

In addition to the attention given the cargo and transfer system, the ship's other systems were studied to further confirm and refine the preliminary hazards study and to get a clear picture of all the interface situations between the cargo system and other ship's systems.

The study team devoted onboard time to the structuring, in preliminary form, of logic trees describing several potential cargo system accidents and to developing the first steps of an HMEA tabulation of cargo system

hazards. Full advantage was taken of being on the ship to check the detailed considerations evoked by the trees and tabular formats of these hazards analysis techniques.

2.4 ANALYSIS AND REPORTING

The safety analysis consisted of carrying out the following steps:

(1) Review and formalization of the top-level accident array pertaining to commercial vessels

(2) Preparation and analysis of logic trees covering the fire and explosion accident situations postulated for the cargo system and pump room

(3) Preparation and analysis of an HMEA for the principal subsystems and components of the cargo system

(4) The construction, based on the above analyses, of a safety critical profile for the STUDY VESSEL's cargo system.

(5) Preparation of a critique on the susceptibility of the STUDY VESSEL to the safety analysis techniques employed giving guidelines for the most effective use of those techniques.

Following the conduct of those analysis steps, the present report was prepared.

3.0 RESULTS

The results of the safety analysis are presented in a format parallel to that of the task objectives stated in Section 1.2, namely, (1) a description of the STUDY VESSEL's SCP for the vessel system/hazard category studied with supportive discussions of inspection data developed, power of the analysis methodologies for generating the intended output, and an analysis of the parameters governing criticality; (2) an appraisal of the study's utility as a demonstration of system safety analysis for a commercial vessel: and (3) identification and definition of needed modifications to VIIS.

3.1 INSPECTION CRITERIA--AN EXAMPLE SCP

The example SCP generated in this study is of limited scope in that it pertains only to inspection activities in the STUDY VESSEL's cargo system with respect to the general hazard of fire and explosion. The techniques used in developing it are judged to be tractable to expansion to all the other vessel systems and all six types of general hazards.

The profile that resulted from this study is portrayed in Figure 1-1 in a screen format to show how the information might be presented to a VIIS user. Its structure is that of a grouped listing. The list is composed of the names of failures for the inspector to attempt to discover using suitable methods of examination and testing. Thus, the nomenclature has been worked out to convey more than merely the name of a thing or subsystem to be inspected. The criterion for inspection action is also implied.

The groups into which the list is divided are the priority catogories that were determined from a criticality analysis procedure discussed in Section 3.4. Although this procedure produces a finer-grained variation than is reflected in Figure 3-1's grouping, it was considered infeasible from the standpoint of practical inspection procedures for the inspector to be able to respond effectively to more than two priority categories above the normally significant list of inspection items.

The items listed in the priority 1 and 2 categories would be stored in VIIS as an explicit part of the information contained in the "Vessel Inspection Critical Profile" segment of the data base. No change in VIIS's design is required to accommodate this.

3.2 INSPECTION RELATED DATA

The data upon which a system safety analysis depends, if quantitative solutions whose numbers have real validity are being sought, are frequency information concerning accident-initiating failures and cost information concerning accident consequences. Of those two categories, the frequency information is the most important. This system safety analysis proved to have these same data needs.

DATE/ _____ VESSEL SAFETY CRITICAL PROFILE PAGE 1 OF 2

ITEM	INSPECTION	HAZARD
	A. MANDATORY INSPECTION ITEMS	
CARGO TANK VENT PIPING	FUNCTION AND MAT COND	OPENINGS INTO TANKS
MAIN CARGO DECK	WASTAGE--PLATING/WELDED FEAT	OPENINGS INTO TANKS
CARGE TANK BULKHEADS	MAT COND RE WASTAGE/CRACKS	NEXT SPACE LEAKAGE
MAIN DECK CARGO PIPING	MAT COND RE WASTAGE/CRACKS	LEAKS TO TOPSIDE AREA
	B. CRITICAL INSPECTION ITEMS	
PUMP RM EXH VENT MOTOR	MECH COND--ELECT INSULATION	SPARK DISCHARGE
PUMP RM EXH VENT TRUNK	MAT COND--WASTAGE/LOOSE OBJ	AIR LEAK--SPARK DISCHARG
PUMP RM LIGHTING	INSTALLATN--BREAKAGE--HOT	HOT SPOT IGNITION SOURCE
PUMP RM PIPING/STRUCT	MAT COND--WASTAGE/CRACKS	INCIPIENT LEAKS
F/FOAM GENERATOR	ADEQUATE FOAM CHARGE	INOPERABLE IN EMERGENCY
--ELECTRICAL EQUIPMENT	FUNCTION--INSULATN--MAT COND	EMERGENCY SERV FAILURE
--PIPING	FUNCTION--FREE OF STOPPAGE	INOPERABLE IN EMERGENCY
--OP INST & MARKINGS	ADEQUATELY PRESENT	INOPERABLE BY PERSONNEL
CARGO TANK ULLAGE FTGS	DAMAGE OR WASTAGE	NONCLOSURE OF TANK
REM VALVE STUFF BOXES	MAT COND--TIGHTNESS	NONCLOSURE OF TANK
CARGO TANK HATCHES	MAT COND--DAMAGE	NONCLOSURE OF TANK
CARGO TANK WIRING	MAT COND--INSULATION	SHORTING--SPARK DISCH

COMMAND/_____ RESPONSE/_____

FIGURE 3-1. SAFETY CRITICAL PROFILE

DATE/ _____ VESSEL SAFETY CRITICAL PROFILE PAGE 1 OF 2

ITEM	INSPECTION	HAZARD
	B. CRITICAL INSPECTION ITEMS (CONT)	
TANK WASH HOSE	ADEQUATE GROUNDING	SPARK DISCHARGE
DRIP PANS	MAT COND--LEAKAGE	LEAKS TO TOPSIDE AREA
FIRE MAIN	MAT COND--OPERATION	EMERGENCY SERV FAILURE
FIRE PUMP	FUNCTION--INSULATN--MAT COND	EMERGENCY SERV FAILURE
CARGO TANK PIPING/VALVS	MAT COND--LEAKAGE	LEAK INTO CARGO TANK

COMMAND/_____ RESPONSE/_____

FIGURE 3-1. (Continued)

No applicable data on the frequency of the accident-initiating failures identified in this study were discovered. The failures were in two general categories: (1) Those creating a barrier-free, combustible fume path such that an ignition could propogate into a closed tank or to a sustaining fuel source and (2) Those providing the requisite ignition. Typical of the first category is the failure "flame arrest screen wasted and ineffective"; of the second is "ungrounded metal objects in space." No records were found where failure frequency information of that kind had been collected. In fact, no significant collection of any failure frequency information for commercial vessels at the component or subcomponent levels of detail are known to exist. For this reason, the analysis was carried out using qualitative techniques. With such techniques, experience and judgement of individuals knowledgeable in the area are used as surrogates for quantitive data.

As will be discussed in the next section of this report, these qualitative techniques produced plausible, consistent results in which it is believed the Coast Guard can have confidence. However, a system safety analysis (or any kind of system analysis) improves in its ability to assist in the making of decisions to the extent that it can be switched to a quantitative basis. Accordingly, one of the important implications of the Coast Guard's adopting a system safety approach as a part of its vessel safety program is that pertinant failure data could conveniently be accummulated in VIIS's central data base over a period of time. The Coast Guard safety analysis program could progressively be switched to this quantitative base. The initial qualitative studies could define the failure data that are pertinent and should be collected thus making the best use of data collecting resources. VIIS, as now designed, is capable of providing the accumulating and organizing capability required and is estimated to have adequate capacity to store the data.

3.3 APPLICABILITY OF THE ANALYSIS TECHNIQUES TO COMMERCIAL VESSELS

The system safety analysis techniques employed in this study were readily and effectively applied to the STUDY VESSEL. Although difficulties in details of techniques were encountered, they were neither greater nor less

than difficulties that Battelle researchers have experienced in adapting system safety analysis techniques to the urban mass transit, railroad, and natural gas pipeline modes of transportation. Several distinct patterns or guidelines for the use of the techniques in connection with commercial vessels emerged.

Three analysis techniques were used in carrying out this study: preliminary hazards analysis (PHA), hazard mode and effect analysis (HMEA), and fault tree analysis (FTA). The last of these was termed "logic tree analysis" in this report as the authors consider this a more accurate descriptive name.* A PHA uses a tabular/textual format to list the main hazards that must be considered with respect to a system and to characterize them in various ways so as to set design criteria, operational safety objectives or, as in the case of the study, the relative effectiveness of various means of controlling the hazards such as the inspection function. An HMEA also uses a tabular format to list hazardous components and subsystem failures and make a systematic investigation of the effects of such failures and their relative criticality. The end purpose of an HMEA is to help guide decisions as to the most effective use of resources in subduing the hazards in the system. Since the analysis logic flow proceeds from the specific (component failures) to the general (system level accident effects) it is properly described as inductive analysis. Logic tree analysis is the reverse; it is a deductive process in which the analyst postulates an undesired system event-- an accident-- as an effect and then explores the possible causes of the event through successive subdivisions of detail until the initating failures that could cause the accident are revealed. The symbolic logic diagram or "tree" is a convenient and powerful form of notation for this mode of analysis. Its end purpose is to reveal the multiple event chains that can cause accidents (the HMEA can only handle single-event accidents) and portray them

---

* The orderly practice of system safety analysis is beset by more-than-usually severe problems of redundant and confusing terminology thought of and applied by various practitioners. A PHA is otherwise known as a "gross hazards analysis", or an "accidental environment analysis"; many authorties point out, with strong justification, that the HMEA is identical to the reliability engineer's failure mode and effects analysis (FMEA); and many workers, including the authors of this report have tried to do away with the unfortunately loaded term "fault tree".

in convenient form for qualitative engineering study. The logic diagram, if properly structured, is also a rigorous, symbolic representation of the mathematical process by which the probability of the top event accident can be calculated given the probability of the root causes. Thus, this form of analysis also lends itself to quantitative studies of hazards and their characteristics.

In the present study the analysis techniques functioned in a manner complementary to each other; each played an essential role in obtaining and supporting the findings. The PHA served to scope the study and provided initial guidance as to the relative significance of the inspection function in controlling fire and explosion hazards in the STUDY VESSEL's cargo system. This is a necessary prelude or first step in any safety analysis. The results of the PHA are considered to be broadly applicable to this class of commercial vessels. It is believed that a standardized set of general hazards and their assessment might be established in the Coast Guard vessel safety program so the PHA would not need to be re-done for each new vessel coming into service.

The HMEA technique was highly effective in focussing on inspection matters since its starting point is a hypothesis about inspectable failures that might occur. However, the HMEA was severely hampered because of its inability to comprehend multiple event accidents--the ones most encountered in considering fire and explosion hazards. On the other hand, the logic tree approach proved highly adept and flexible in dealing effectively with this kind of complexity. The logic tree approach seemed to the authors considerably more powerful a tool for identifying the root cause conditions in initiating accidents and comparing their criticality. The main detriment associated with logic tree analysis was that it is inherently overly comprehensive--the analyst finds himself studying matter not germane to his problem in order to construct a good logic tree for an accident. The logical rigor imposed by the tree construction process makes the analyst's job demanding and expensive both as to professional staff cost and time costs. Any decision made to employ a logic diagram analysis should be made recognizing this cost increment over other forms of safety analysis.

As noted in the previous section, all analysis techniques were applied in an essentially qualitative way because of the sparseness of relevant data. This consideration plus those discussed in the foregoing led to the following tentative guidelines for conduct of system safety analyses with commercial vessels:

(1) Always conduct a PHA as a first step to scope the exercise, define the accident types to be considered, identify the interfaces involved, and define the main hazards to be dealt with.

(2) Utilize the accident logic diagram as the principal analytical technique so the strategy of the study is essentially deductive. Complement this with HMEA examinations of subsystems and components.

(3) Be willing and prepared to proceed with qualitative analysis techniques as illustrated in this study.

(4) Scope studies carefully to avoid excessive labor. Properly applied, the techniques work well with limited scope because they handle interfaces effectively. It is not necessary to study a complete vessel if one is concerned only with the cargo system.

3.4 CRITERIA FOR CRITICALITY

The "criticality" at issue in this study is the relative importance of inspecting for a given failure. The criticality analysis sought to answer the question "given a number of failures that could cause accidents at various levels of severity, which is the most important to inspect for, which next, and so on?" The failures referred to are not accidents. They are failures of equipment or structure which could lead to an accident in service. In this context, shell plating wasted to less than the minimum allowable thickness would be such a failure.

In the present study, the following criteria were found to be significant to assessing the criticality of inspecting for a failure.

- Hazard Severity. The relative severity of the consequences of the accident that would result from activation of the hazard. A hazard severity classification scheme was developed during this study and is described in the section covering the conduct of the preliminary hazard analysis. The higher the severity the greater the criticality.

- Impact of Inspection on Failure Probability. The degree to which the inspection process can favorably alter the probability of occurrance of the failure. This basically has to do with how much control the inspection process is able to exert over the hazard by discovering the failure and getting it restored. The assessment depends on how long, with respect to the inspection interval, the restoration is expected to last. A ullage cap found improperly installed by an inspector may be corrected on the spot but then it may be used and reinstalled improperly again the next day. On the other hand, a vapor leak path caused by a badly corroded weld joint at a tank penetration would be restored by welding new material in place--a restoration that should last a matter of years, well beyond the interval to the next inspection. In the former case the inspection process has exerted almost no control over the hazard involved whereas in the latter case virtually complete control has been obtained. The criterion should be applied so that inspection effort is spent first on high control effectiveness items.

- Combinations Required. The failure combinations required to initiate the accident. Some failures can precipitate the accident of concern by themselves; these are termed "single-failure" accidents. In other cases, the failure cannot by itself cause the accident; some other one must occur at the same time. For example, a fire requires the simultaneous presence of a combustable vapor (a failure of some kind causing a leak) and a source of ignition. These are termed "two-failure" accidents. A two-failure accident is less probable than a single failure accident hence failures in the single failure class are considered more critical to inspect for than those in the multiple failure class.

These three criteria were used qualitatively in arriving at the SCP presented in the foregoing section. The criteria are mixed in that some are keyed to safety considerations whereas others are related to matters of effectiveness in use of inspection resources. In applying these criteria the project team weighed them uniformly.

3.5 UTILITY OF THIS STUDY AS A DEMONSTRATION

This study is considered to have served its purposes adequately as a demonstration. The applicability of system safety analysis techniques to commercial vessels has been shown; their ability to generate an SCP has been confirmed; and their probable impact on the design of VIIS (to be covered in the next subsection) has been measured. The demonstrations as to these matters are considered credible by the research team.

There was some concern about the study's usefulness when it became apparent to the study team that the hazards identified in the course of the work did not include new or unsuspected ones of significance. It had been expected at the outset that the investigation would turn up some interesting surprises, thereby lending credence to the claim that systems safety analyses are capable of spotting hazards in novel technology systems where no accident history is available; that such surprises did not materialize had the effect of an anticlimax. For a time, this obscured the significance of the study's main result--the development of a structured, prioritized recitation of detailed fire/explosion hazards in the STUDY VESSEL's cargo system which spans and goes beyond the experience base on hazards in this type of vessel. It was developed through the rigorous use of system safety analysis techniques. The fact that it effectively captures what experience and expertise would be able to offer using traditional approaches to safety assurance is considered strong testimony to the efficacity of the system safety approach in identifying hazards.

This is not to say that this study is a candidate to serve as a reference work upon which to base the implementation of system safety analysis procedures in the Coast Guard's vessel safety program. It cannot do that because of its limited scope (one casualty type, one ship system, and one ship). A body of work encompassing a much greater range of example analyses would be required to perform the basic reference function effectively. The entire accident spectrum should be investigated for all the systems in several vessels representing the principal types in commercial service. A vessel system safety study carried out in a scope of this magnitude could result in a comprehensive documentation of example safety analysis exercises for commercial vessels. Such documentation would provide direct guidance for investigations the Coast Guard might wish to conduct internally; it could be referenced in situations in which the Coast Guard might specify that a vessel system safety study be conducted by others as a means of compliance with a safety requirement.

3.6 POTENTIAL IMPACTS ON VIIS

The results of the safety analysis are expected to affect the design of VIIS in three ways.

First, the system must provide capability for entry, update and retrieval of an SCP for each vessel in the system as appropriate. This amounts to the addition of one more "product" to those already provided in the system. VIIS has been designed with the flexibility to add and delete products of this kind without any impact on the system's software or hardware.

Second, the system must be able to accumulate failure data from the field in the manner noted in the discussion in Section 3.2. The capability for performing this function is already incorporated in the VIIS design as the Vessel File Damages/Defects Log.

Third, it may be found advantageous, if system safety practices become a part of the Coast Guard's vessel safety program, to incorporate the capability to solve logic trees in VIIS. Such a capability would become an integral part of the system's array of analysis programs. Note that this capability would probably not be of direct usefulness in the inspection program. Rather, it would be exercised in connection with plan review activities.

A discussion of how the VIIS implementation plan should be modified to incorporate the above features is included as Appendix C.

4.0 SYSTEM SAFETY ANALYSIS

The purpose of any system safety analysis procedure is to assist in determining the most effective use of available resources to assure the safe operation of the system involved. In this case, the "system" is the STUDY VESSEL and the available resources consist of the Coast Guard's inspection function--its personnel, facilities, and regulatory authority.

The inspection function can affect directly only the materiel condition of the ship; consequently, of all the accidents that might occur to the STUDY VESSEL, only those triggered by materiel failures can be

prevented through inspection. This is the inherent scope of inspection's capacity to assure safe operation of the system. Inspection cannot prevent accidents occurring because of crew mistakes in operating or navigating the vessel nor can it prevent accidents caused by inadequacies in the vessel's original design. In fact, the most apt description of the inspection function's hazard control scope is that it operates on those hazards arising due to the vessel's going in any manner to an off-design materiel condition. Note further that this process is necessarily discontinuous--the effective inspection interval is on the order of six months to a year--so off-design degradations are permitted by the process. The severity to which they are allowed to develop is limited by the inspection interval.

Within this field of action, then, the purpose of system safety analysis is to help choose the inspection procedures that will make the most effective use of the inspector's time and the Coast Guard's regulatory authority in controlling hazards. This is an optimization objective the recognition of which led to the concept that the specific failure items to be inspected for on the STUDY VESSEL could be rank-ordered by a criterion of importance for inspection. This concept, in turn, led to the idea of structuring the safety critical profile for the vessel as discussed previously.

Three safety analysis techniques were employed: (1) preliminary hazards analysis, (2) logic diagram analysis, and (3) hazard mode and effects analysis. Using the results of these studies, an inspection criticality criterion was formulated and the inspection items were rank-ordered using it. Finally, the safety critical profile was developed.

Preceeding the conduct of these analyses, an examination of the commercial vessel accident environment was carried out as a separate step to scope the subsequent studies and define the types of accidents to be considered.

4.1 THE COMMERCIAL VESSEL ACCIDENT ENVIRONMENT

The accident environment in which the STUDY VESSEL functioned was examined first in general terms--a review of all the types of accidents

that might occur--and then specifically for the purpose of choosing the accidents and systems to be analyzed in detail. The accident environment is portrayed symbolically in Figure 4-1. The environment was visualized as a three-level tree in which each level shows more detailed subdivisions of basic accident types. In doing so, the tree also implies the categories of parties-at-risk with respect to each accident type. These accident and parties-at-risk categories were based on traditional definitions evolved in Coast Guard usage over the years of its operational responsibility for marine safety matters. In connection with this study, the definitions of the categories were reviewed and updated to ensure that they cover all the accidents and risk areas that could conceivably pertain to the STUDY VESSEL and her general class.

The diagram was drawn with logic symbology because it forms the top level of accident analysis trees that were developed later in the safety study. The alphanumeric locators designate "events", as described in the rectangular boxes, and "logic gates" as symbolozed in the OR symbols. The meaning and use of this symbology is covered in Appendix D of this report. For the present discussion, the figure's significant meaning lies in the party-at-risk categories and accident class subdivisions it portrays.

4.1.1 Party-at-Risk Categories

In the Coast Guard's domain of responsibility, there are three impact groups or parties-at-risk that are hazarded by the kinds of accidents that might occur to the STUDY VESSEL. They were defined more precisely in the following terms:

- Public-at-Risk. This category includes risk to the life and well-being of members of the general public; risk of damage or loss to public property; and risk of damage to the marine environment.

- Vessel-at-Risk. This category includes the risk that an accident will result in damage to or loss of the vessel and/or her valuable cargo.

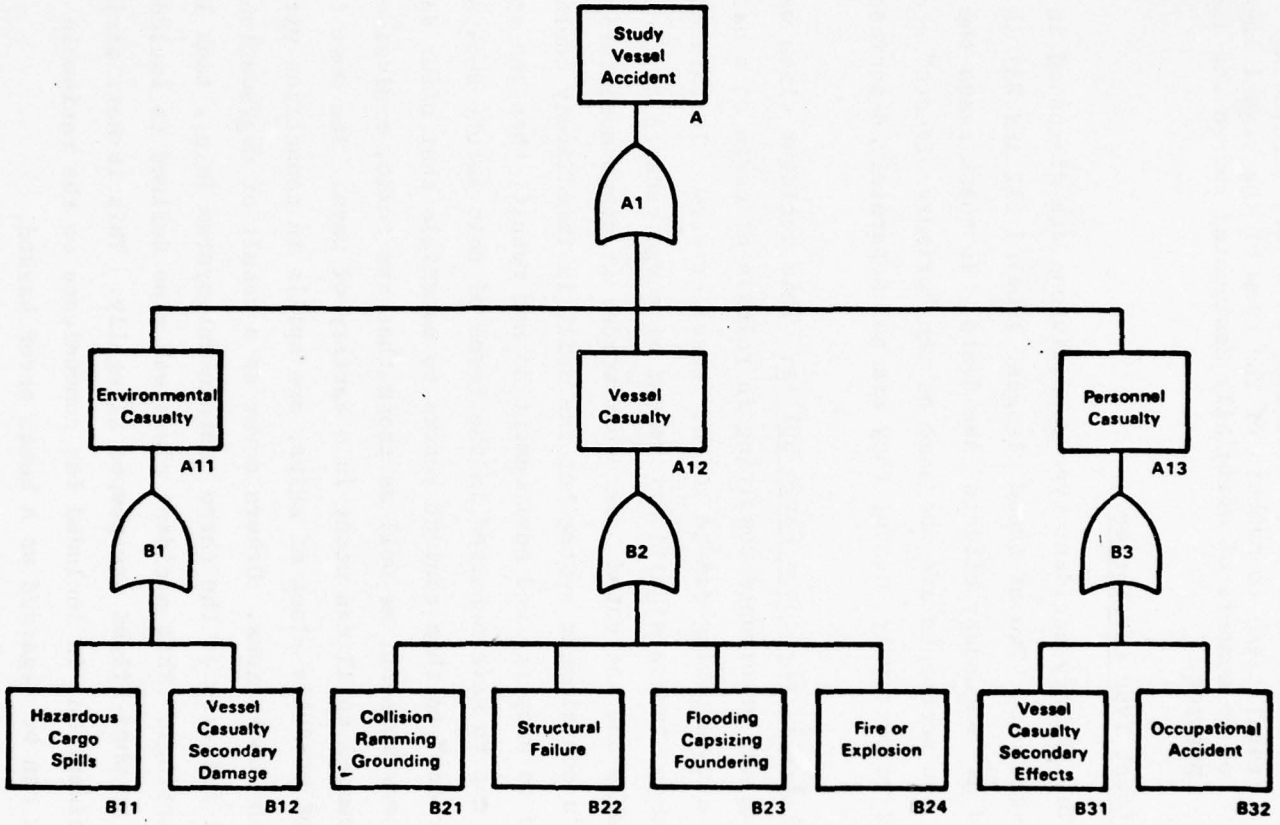


FIGURE 4-1. LOGIC DIAGRAM PORTRAYING THE COMMERCIAL VESSEL ACCIDENT ENVIRONMENT

- Crew-at-Risk. This category includes the risk that an accident will occur resulting in injury (including fatalities) to members of the crew of the vessel involved or to members of officially designated rescue and aid parties.

4.1.2 Accident Type Categories

The primary accident type subdivisions are discussed in the following subsections. Two of these classes, labeled B12 and B31 in Figure 4-1 are classed as "secondary effects" accidents. In these cases the final results of the accidents are the same as the "primary effects" accidents B11 and B32 respectively, hence, they are not separately described.

4.1.2.1 Hazardous Cargo Spills. This accident class was defined as including any occurrence resulting in release of cargo of a hazardous nature but not involving damage to the vessel or crew. In this context, "release" means that a significant amount of cargo escapes any control measures available and activated. In other words, if cargo momentarily escapes the vessel's containment system but the spill is immediately contained so that damage to property and environment do not result, then the spill is considered not to have occurred in the terms of this safety analysis. The term "hazardous" in this context refers to materials that offer damage to the marine environment, as well as those that are toxic, explosive, etc. An intact vessel spill can occur in a variety of ways. The most frequent, in the STUDY VESSEL's class of ships, are spills in connection with loading and unloading operations. Others occur as a result of degradation or operational failures of the cargo containment system (e.g., tank leak at a corroded fitting). This accident class was also defined to include intentional discharges as when bilges are pumped illegally. This is not, strictly speaking, an accident but is included for convenience on the rationale that an illegal act can be regarded as a human error hazard.

4.1.2.2 Collision, Ramming, Grounding. This is the class of accidents where as a primary event, the vessel strikes another object. "Collision" refers to striking another vessel. "Ramming" means striking another object, such as a pier, that is not a vessel. "Grounding" refers to events where the vessel contacts the bottom or the shore.

4.1.2.3 Structural Failure. This accident type includes all circumstances where a vessel experiences major structural failure as a primary event. A vessel's breaking up in heavy seas due to overstressing the hull strength members is an example.

4.1.2.4 Flooding, Capsizing, Foundering. This accident type involves a vessel's losing buoyancy or stability or both as a result of primary events such as loss of watertight integrity or incorrect cargo load distribution. As a primary event, this type is rare; it more frequently occurrs as a secondary event after collision, ramming, grounding, or structural failure.

4.1.2.5 Fire or Explosion. This accident type includes any situation aboard the vessel where an ignition propogates explosively or to a sustained supply of fuel to form a fire.

4.1.2.6 Occupational Accident. This is any accident aboard the vessel causing injury or death to crew members but not caused by a vessel casualty.

4.2 PRELIMINARY HAZARDS ANALYSIS

As discussed in Section 3.3, the purpose of a PHA in a safety analysis, is to list the main hazards that should be considered with respect to a system and characterize or classify them in a variety of ways in order to set design criteria, define operational safety objectives, or, as in the case of this study, to investigate the relative effectiveness of various means of controlling the hazards. The means in which there is the greatest interest here is inspection. Others are: improved design, special operating procedures, etc.

In this case, another special purpose of performing a PHA was to confirm the tentative decision to concentrate the later detailed safety analysis effort on the STUDY VESSEL's cargo system and the accident category "fire and explosion". The tentative decision was based on the current

importance of the cargo system--especially the pump room part of it--to the Coast Guard's safety program. The PHA was able to help re-examine that decision in the context of the complete hazard picture for the STUDY VESSEL.

4.2.1 PHA Technique

The PHA utilizes a tabular/textual format of great flexibility. As long as a broad hazards-listing approach is taken, there are few other prescribed factors to be taken into account in setting up the analyses. The investigator is free to identify and tabulate those aspects of the hazards that best serve his purpose. In this study, seven such aspects were assessed.

4.2.1.1 Vessel Operating Phase. Many of the hazards are "active" --can become accidents--only during certain of the vessel's operating cycle phases. For example, it is unreasonable to suppose that the STUDY VESSEL would capsize, as a primary accident, while unloading cargo at the pier. Further, the severity of the consequences of all the types of accidents considered varies markedly from one operating phase to the next. It would be worse to have a major explosion while tied up at the pier unloading near large population centers than while several hundred miles at sea so only the vessel and crew are hazarded. Accordingly, the STUDY VESSEL's operating cycle was broken down into phases and the hazards analysed with respect to each of the phases. The phases chosen for the STUDY VESSEL are listed in Appendix A.

4.2.1.2 Hazard Activation Modes. The circumstances which must exist in order to activate a hazard reveal much about how that hazard can best be controlled and, of interest here, the relevance of inspection to controlling it. Data required to fill out this column concern the types of failures, omissions, design deficiencies, and the like that can be conceived of to bring about the accident.

4.2.1.3 Relative Frequency of Accident Type. This factor assessment measures the level of historical occurrence of the accident type in the vessel class. There are some statistics collected on this topic so a quantitive assessment could theoretically be made. However, each of the hazards considered in the PHA is being considered as a "primary" hazard--

the accident being assessed does not occur as a secondary effect to some other casualty. Available data collections on vessel casualties are confusing in this respect; many chain-type casualties are indexed to their secondary or tertiary accident types instead of the primary. Also, the published information is not broken down by operating phase. Therefore, a considerable amount of judgement must go into the making of this assessment and the measures chosen for entry in the table are not quantitive ones.

4.2.1.4 Potential Accident Effects. This assessment column indicates the expected effects of the accident type under consideration. In making this assessment, the probable secondary and tertiary consequences of the primary accident event are taken into account. For example, if the accident event being considered is "collision", the potential effects assessment recognizes that, in all probability, a collision involving the STUDY VESSEL would result in a major spill of hazardous cargo, since cargo tanks would probably be breached as a secondary consequence of the collision. In assessing potential accident effects, the structure of the parties-at-risk concept discussed earlier was taken directly into account.

4.2.1.5 Hazard Category. This characteristic recognizes that the hazards under consideration do not have the same potential for damage and loss. Some are more severe in this respect than others. The idea of there being a gradient of severity among hazards is one of the most important bases of the whole system safety approach; the most important of the primary reference documents codifying the ideas of system safety, MILSTD 886, prescribed early a scheme for representing the different severity levels hazards can have. That scheme has been adapted by this project team to the context of commercial vessel safety. The different categories and their meaning are shown in Table 4-1.

TABLE 4-1. HAZARD CATEGORIES

CATEGORY	RANKING	CONSEQUENCES
I	Negligible	No damage, loss or injury resulting from accident.
II	Marginal	Accident effects can be controlled without damage, loss, or injury.
III	Critical	Accident potential effects, loss and/or injuries can be controlled only by immediate corrective action
(A)		--Involving vessel and crew only
(B)		--Involving vessel and crew plus environmental damage
(C)		--Involving vessel, crew, environmental damage plus public property damage/loss and injuries/fatalities to members of the public
IV	Catastrophic	Uncontrollable major damage and injuries/fatalities
(A)		--Involving vessel and crew only
(B)		--Involving vessel and crew plus environmental damage
(C)		--Involving vessel, crew, environmental damage plus public property damage/loss and injuries/fatalities to members of the public

4.2.1.6 Degree of Inspection Control. This characteristic has to do with the net amount of control over the hazard exerted by the inspection process. By "control" is meant (1) the degree to which the inspection process can detect the failures or hazardous conditions that could lead to the accident, coupled with (2) the degree to which the results of an inspection can effect a complete removal of the hazardous condition for at least the interval of time before the next inspection. For example, a fire might potentially result in the STUDY VESSEL from vapor leakage from a cargo tank. A leak path might exist because a crew member didn't tighten the hatch properly from the last tank cleaning operation. On the other hand, it might exist because of wasted deck tank top plating in way of a penetration. In the former case the inspection process exerts virtually no control over the hazard as far as that failure is concerned--even if the inspector were able to detect it and get it restored, it might be installed incorrectly

again the day after the inspection took place. In the latter case, however, the failure would be readily detectable and would be restored by welding new material in the place--a permanent repair lasting a matter of years, well beyond the inspection interval.

The assessment of this characteristic for each hazard in the PHA was made using the following ranking parameters.

Weak--------materiel degradation is a zero or minor contributor to hazard actuation. Also, materiel degradation is of small importance to accident effects mitigation or containment. The hazard control picture is dominated by use of fail safe or high-reliability devices and/or use of special procedures by operational crews.

Medium------materiel degradation accounts for only a portion of the conditions that could activate the hazard or mitigate its effects.

Strong------materiel degradations amenable to permanent repairs are the major potential causes of activating the hazard.

4.2.2 Study Vessel PHA

The results of the PHA conducted on the study vessel are shown in the tabulation in Figure 4-2. Several significant insights about the role and pertinance of the inspection function were drawn from these results.

- With respect to primary hazards, the inspection function is of greatest importance for controlling the structural failure hazard, and of considerable importance for the flooding-capsizing-foundering and fire and explosion hazards. It has little control significance with collision-ramming-grounding, intact vessel spills, and occupational accidents.

- Since both structural failure and fire and explosion are frequently-occurring secondary hazards--following collisions--the inspection function takes on added importance for effects mitigation.

- The hazard picture for commercial vessels of the STUDY VESSEL's class is severe. Nearly all of them were category IV hazards threatening more than one of the parties-at-risk in all vessel operating modes assessed.

- The most severe overall hazard condition exists when the vessel is loading or proceeding loaded in or out of harbor. Next most

Primary Hazard	Vessel Operating Phase	Hazard Activation Modes	Relative Frequency in Vessel Class	Ship Systems Involved - Primary - Secondary - Etc.	Potential Effects	Hazard Category	Degree of Inspection Control	Remarks and Methods of Control
Hazardous cargo spills	Loading or unloading cargo at dock	Failures and/or management errors in controlling cargo transfer system	High	- Cargo transfer system	• Environment damage • Public property damage	IIIB	Weak	Hazard control dominated by high-order personnel training and adherence to procedures.
Collision ramming grounding	Entering or leaving port with cargo loaded	Failures and/or errors in vessel control and maneuvering systems	High	- Hull - Cargo system	• Vessel damage or loss • Public property damage • Personnel casualties • Environment damage	IVC	Weak	Control is exerted mainly through safety devices (navigation equipment) and special procedures involving special skill and judgment.
	Cruising at sea loaded	Ditto	Medium	Ditto	• Vessel damage or loss • Personnel casualties • Open sea spill	IVB	Weak	Inspection's role is to ensure presence. operability, and accuracy of equipments involved.
	Cruising at sea in ballast	"	Medium	- Hull	• Vessel damage or loss • Personnel casualties	IVA	Weak	
Structural failure	At sea, loaded, heavy weather	Hull strength degradation	Low	- Hull - Cargo system	• Vessel loss • Personnel casualties • Open sea spill	IVB	Strong	Basic hazard control is correct structural design. Inspection's prime role is to ensure degradation from design conditions is not excessive.
	At sea, in ballast, heavy weather	Ditto	Medium	Ditto	• Vessel loss • Personnel casualties	IVA	Strong	

FIGURE 4-2. PRELIMINARY HAZARDS ANALYSIS

Primary Hazard	Vessel Operating Phase	Hazard Activation Modes	Relative Frequency in Vessel Class	Ship Systems Involved - Primary - Secondary - Etc.	Potential Effects	Hazard Category	Degree of Inspection Control	Remarks and Methods of Control
Fire and explosion	Loading cargo at terminal near population centers	Combustible mixture escape joined with ignition source	Moderate	- Cargo system - Hull	• Vessel loss • Personnel casualties • Environment casualty • Public property	IVC	Moderate	Principle method of control is to deny ignition source and/or flame front path to fuel.
	Unloading cargo at terminal near population centers	Ditto	Moderate	- Cargo system (incl. pump room) - Hull	Ditto	IVC	Moderate	Method of control the same. Only difference is involvement of pump room
	Underway, loaded, on soundings (entering or leaving harbor) near population centers	"	Low	- Cargo system - Propulsion - Habitability	"	IVC	Moderate	Inspection's role in controlling this hazard is classed as "moderate" because it figures mainly in mitigation of effects rather than prevention. The adequate presence and condition of fire-fighting equipment is a prime function of inspection. Inspection is also important in forestalling leaks of combustible mixtures. Denial of ignition is almost completely dependent on procedures
	Underway, in ballast, on soundings	"	Low		• Vessel loss • Personnel casualties • Public property	IVB	Moderate	
	Underway, at sea, loaded	"	Low	- Propulsion - Cargo system - Habitability	• Vessel loss • Personnel casualties • Open sea spill	IVB	Moderate	

FIGURE 4-2. (Continued)

Primary Hazard	Vessel Operating Phase	Hazard Activation Modes	Relative Frequency in Vessel Class	Ship Systems Involved - Primary - Secondary - Etc.	Potential Effects	Hazard Category	Degree of Inspection Control	Remarks and Methods of Control
Fire and explosion (continued)	Underway, at sea, in ballast	Combustible mixture escape joined with ignition source	Low	- Propulsion - Habitability	• Vessel loss • Personnel casualties	IVA	Moderate	
	Underway, at sea, unloaded, tank cleaning/ preparation operations	Ditto	Medium	- Cargo system - Propulsion - Habitability	• Vessel loss • Personnel casualties	IVA	Moderate	
Occupational accidents	All	• Defective industrial equipment • Unsafe working procedures	Medium	All	• Personnel casualties	IVA	Weak	Hazard control dominated by training factors and inculcation in proper procedures.

FIGURE 4-2. (Continued)

severe is unloading. The main influencer here is the condition of hazardous cargo being close to population centers. The most hazardous condition for the vessel and crew at sea is when tank cleaning operations are being carried out during the southbound voyage.

4.2.3 Selection of Scope for More Detailed Safety Analyses

The hazards picture drawn by the PHA strongly supported the tentative decision made earlier to perform the more detailed safety analyses steps on the STUDY VESSEL's cargo system and deal only with the primary hazard "fire and explosion". The need to limit the detailed studies to some such scope had been recognized from the outset of the program--there were not enough resources to conduct a safety analysis of the entire vessel. The tentative scope selection was based on recognition of the current criticality to the Coast Guard of hazardous cargo related casualties--especially those causing spectacular fires. The only concern on the point stemmed from the question of how strongly the inspection function bore upon that accident class in that vessel system. The PHA showed a strong but not dominant role for inspection. This was accepted as being a satisfacotry situation for pursuing the objectives of this research task.

4.3 LOGIC DIAGRAM ANALYSIS

The logic diagram analysis began with event B22 in the top level tree shown in Figure 4-1. The tree was developed down from this event through the C and D levels in order to identify the specific accidents of concern in this analysis. Figure 4-3 shows this development and also repeats the complete top level diagram for convenience. Correct symbology is used in this portrayal of the diagram to indicate the branches being developed in this analysis. A discussion of how the logic diagrams are constructed giving explanations of the symbols used is given in Appendix D.

The rationale behind the C-level development is that the ship systems most vulnerable to the fire and explosion hazard are those where significant amounts of combustible materials (fuel oil, combustible cargo, bedding, clothing) and ignition sources (flames, hot metals, cookstoves)

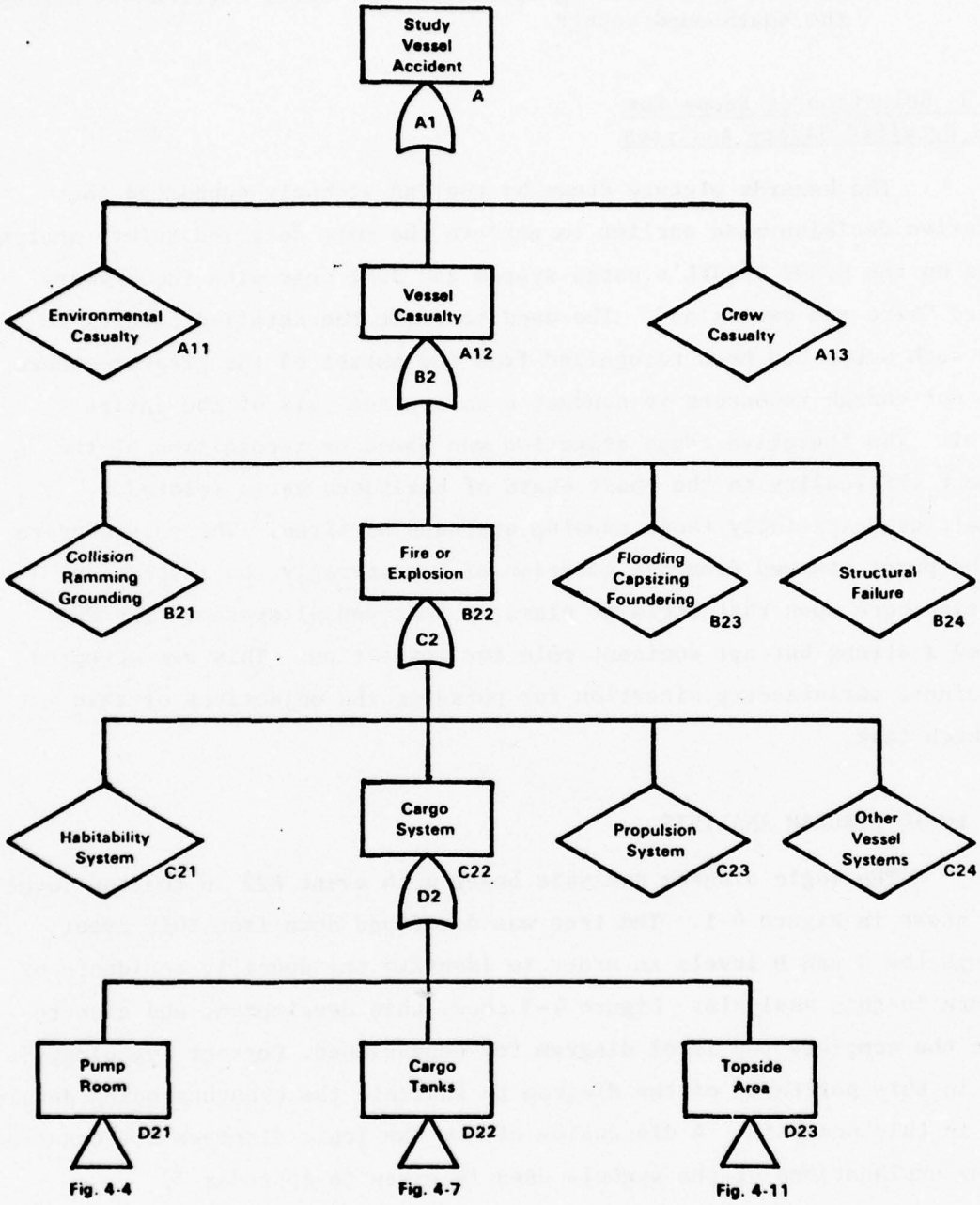


FIGURE 4-3. UPPER LEVELS OF THE FIRE AND EXPLOSION DIAGRAM

are normally present. Three of the STUDY VESSEL's systems were judged to be in this category and therefore would merit individual attention in analyzing the STUDY VESSEL's potential for experiencing fire and explosion accidents. The three are identified in the diagram using symbology to indicate that, in accordance with the scope decision discussed previously, only the cargo system branch, event C22, will be developed further. The balance of the vessel's systems are collected as a single event, C24, to provide a path for analysis of any of them should this prove significant to the problem.

The D-level development indicates how the cargo system in the STUDY VESSEL was subdivided in considering its susceptability to fires and explosions. The pump room is a clearly separable part of the cargo system; all the fire and explosion events which could potentially occur within the physical confines of the pump room space will be developed from this event, D21. Event D22 is defined to include all fire and explosion accidents occurring within any of the STUDY VESSEL's cargo tanks or adjacent cofferdams. Event D23 was defined to include fires and explosions occurring in conjunction with combustible cargo's being spilled on the main deck or over the side and then being ignited in some way. This subdivision of the cargo system of the STUDY VESSEL is intended to be comprehensive, that is, all elements of the vessel's cargo system are intended to be included in one of the three named subdivisions. For example, the vent and main deck piping systems are included as a part of the "cargo tank" event for the purposes of this analysis.

The diagram is truncated at the D-level with symbols indicating the Figure number in this report where the development of each event is continued. As the development of the logic diagrams continues to greater levels of detail, a large number of failures and hazardous conditions will be identified at the roots of the trees. These failures and conditions are hypothetical only. They were identified as possibilities by the study team using analytical and conceptual processes. The failures and hazardous conditions were not observed to exist on board the STUDY VESSEL.

4.3.1 Pump Room Fires and Explosion Study

The development of the pump room branch of the diagram was based

on the study team's conceptualization of the ways in which such events could occur. In addition to the physical familiarization with the pump room and its equipment that was acquired during the voyage, the team reviewed reports of pump room casualties which have occurred in the past, studied the provisions in the CFR 46 Subchapter D, the appropriate sections in the Coast Guard Manual and the Tanker Safety Guide, and conferred on pump room operations and safety practices with appropriate individuals in the STUDY VESSEL's crew. With this body of information in hand, the development of the pump room accident diagram was carried out as a creative design effort.

Basic to the structure of the D21 diagram was the team's recognition that the pump room could be analyzed independently of the different phases of the STUDY VESSEL's operating cycle. The pump room is fully functioning during the cargo unloading phase but it is used almost as much during the southbound cruise in connection with ballast management and tank cleaning/preparation activities, and it is frequently activated for miscellaneous purposes during the other phases of vessel operation. Furthermore, the basic hazardous condition in the pump room--the presence of cargo liquids in the bilges--is physically independent of the vessel's operating cycle. Therefore the pump room analysis is established on a continuous operation basis.

The hazardous condition in the pump room is not complicated. There is generally a certain amount of vapor present because of bilge accumulations --it can get into the explosive concentration range under a variety of conditions. If an ignition source is permitted in the vicinity of such vapor, a flame front may develop which could propagate as an explosion, if there is enough mixture dispersed throughout the volume of the pump room, or it could find its way to a supply of fuel so as to sustain a fire. The STUDY VESSEL's pump room is equipped with a fixed foam system which, if activated in time, could put out the fire quickly. If this does not happen for some reason so that the fire is allowed to burn long enough to cause damage and interrupt operations, then the accident defined in event D21 has occurred.

The above discussion describes a three-path AND'ed condition. The diagram developed from event D21 was built with this basic structure as portrayed in Figure 4-4. This part of the diagram shows the three conditions necessary for a fire or explosion to develop and also shows the development of event E11 "source of ignition present". This development, and the two others, are discussed in the following subsections.

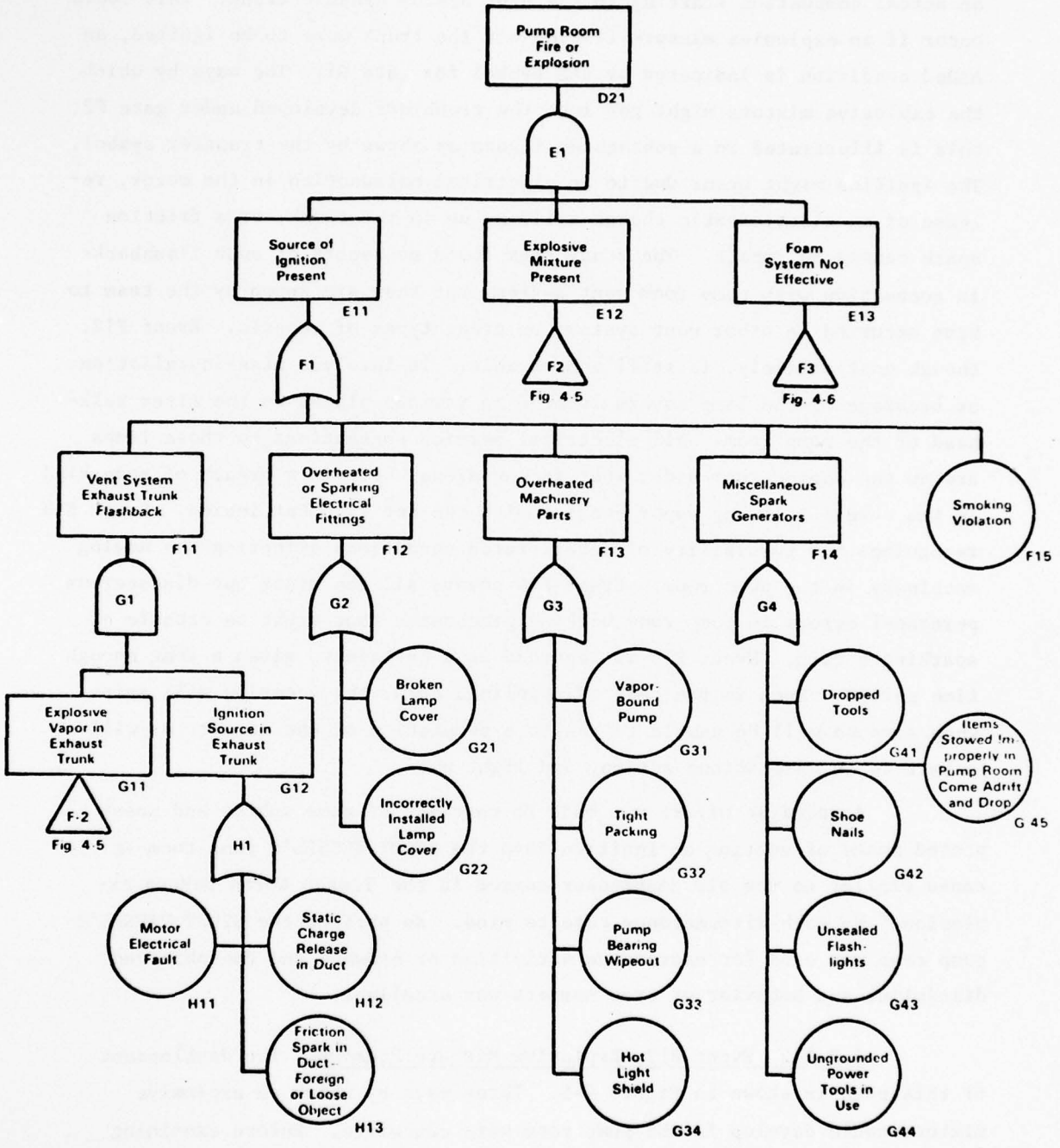


FIGURE 4-4. EVENT PATH D21-E11 DEVELOPMENT--"SOURCE OF IGNITION PRESENT"

4.3.1.1 Event E11, Source of Ignition Present. Five means for getting an ignition source into the pump room were conceived. Event F11 envisions an actual combustion starting in the vent system exhause trunk. This could occur if an explosive mixture flowing out the trunk were to be ignited, an ANDed condition is indicated by the symbol for gate G1. The ways by which the explosive mixture might get into the trunk are developed under gate F2; this is illustrated in a subsequent figure as shown by the transfer symbol. The ignition might occur due to an electrical malfunction in the motor, release of an electrostatic charge building up in the trunk, or a friction spark caused by impact. The study team found no record of such flashbacks in connection with pump room vent systems but they are known by the team to have occurred in other vent systems on other types of vessels. Event F12, though most unlikely, is still conceivable. It involves miss-installation or breakage of the lamp covers located in various places on the after bulkhead of the pump room. All electrical service connections to those lamps are on the engine room side; what is envisioned here is a breach of some kind in the covers allowing vapor contact with the hot filament inside. Event F13 recognizes the possibility of deteriorated conditions affecting the moving machinery in the pump room. Event F14 covers all the minor but disasterous personnel errors in pump room working procedures that might be capable of sparking a fire. Event F15 is regarded as a certainty, given a long enough time period. Even in the best disciplined crew, the occasion will arise when someone will be unable to resist a temptation of the moment, or will submit to an unconscious action, and light up.

A specific effort was made to conceive of some subtle and unexpected means of getting an ignition into the STUDY VESSEL's pump room--a cause similar to the air compressor source in the Texaco North Dakota explosion.* No such circumstance came to mind. No part of the STUDY VESSEL's pump room was used for extraneous activities or stowage and the observed discipline and behavior of crew members was excellent.

4.3.1.2 Event E12, Explosive Mixture Present. The development of this path is shown in Figure 4-5. Three ways by which an explosive mixture could develop in the pump room were conceived. Before examining these, one should note that there is some amount of vapor present most of the time in the lower part of the pump room. To be hazardous with respect to fire or explosion, the vapor must build up to a concentration

* "MARINE CASUALTY REPORT--Tankship TEXACO NORTH DAKOTA, Pump Room Explosion, Gulf of Mexico, October 3, 1973", Report No. USCG/NTSB-MAR-75-5, National Transportation Safety Board, September, 1975.

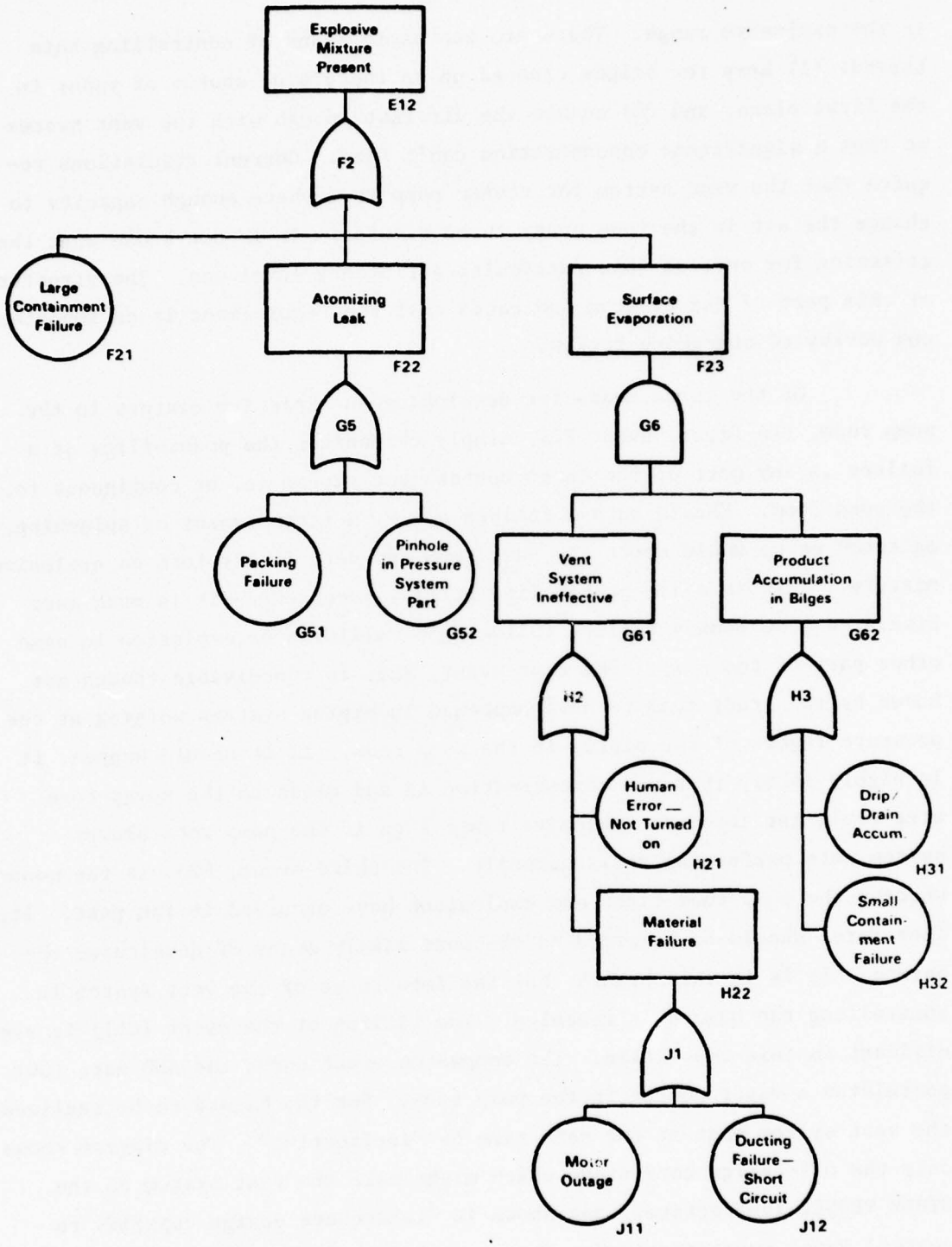


FIGURE 4-5. EVENT PATH E12 DEVELOPMENT--"EXPLOSIVE MIXTURE PRESENT"

in the explosive range. There are two basic means of controlling this hazard: (1) keep the bilges cleaned up so there's no source of vapor in the first place, and (2) change the air fast enough with the vent system so that a significant concentration can't form. Current regulations require that the vent system for tanker pump rooms have enough capacity to change the air in the room every three minutes. It is not known what the criterion for setting this particular stringency level was. The structure of this part of the diagram indicates that the requirement is an important one worthy of searching review.

Of the three means for developing an explosive mixture in the pump room, the first, event F21, simply recognizes the possibility of a failure in any part of the cargo containment system in, or contiguous to, the pump room. Should such a failure occur, a large amount of splashing, agitated cargo would enter the pump room and very likely form an explosive mixture. This is a low-probability primary occurrence--it is much more likely as a secondary failure following a collision or explosion in some other part of the ship. The next event, F22, is conceivable though not known by the study team to have happened in piping systems working at the pressure levels of the piping in the pump room. If it should happen, it is highly likely that the concentration in and close to the spray cone area would get into the explosive range even if the pump room blower system were performing satisfactorily. The third event, F23, is the means whereby the pump room fires and explosions have occurred in the past. It, therefore, should be regarded as the most likely means of developing the hazard. It is in this branch that the importance of the vent system in controlling the hazard is revealed. The titling of the event (G61) is significant in this connection. The companion event under the AND gate (G6) postulates a vapor source in the pump room. For the hazard to be realized, the vent system must at the same time be "ineffective". The diagram shows only the off-design conditions which might make the vent system on the STUDY VESSEL ineffective. Not shown is "inadequate design capacity to control vapor concentration". The question of design adequacy is beyond the scope of this study but the authors believe the validity of the three-minute air-change specification should be reviewed because of the evident importance of the vent system to the control of the pump room hazards.

4.3.1.3 Event E13, Foam System Not Effective. The foam system is intended to suppress fires in the pump room--it can do nothing about an explosion. The meaning of "effectiveness" in this event statement is the capability to put a pump room fire out very quickly after the fire starts--before any damage of significance can have occurred. Figure 4-6 shows the development of event E13 which postulates ineffectiveness of the foam system.

There are two ways whereby the foam system can fail to work. The first, event F31, is a materiel failure of some kind. The three possibilities which the study team conceived of are shown. Innumerable electrical failures are possible; that branch was not developed to the primary level. The second means of failure would simply be that the system is not activated in time to be of service in controlling the fire. The different ways this could happen all fall in the human error category.

4.3.2 Cargo Tank Fires and Explosions Study

The hazard of fires and explosions with respect to the STUDY VESSEL's cargo tank is made up of the same ingredients as in the pump room; namely, cargo vapor in the tank gets into the explosive mixture range and then an ignition source is introduced into the mixture. In most cases, in the confined volume of a cargo tank, this will result in an explosion followed by fire. However, for hazards analysis purposes, it is not necessary to be able to forecast the precise nature of the combustion's outcome. It is defined to fall in the catastrophic range of severity in any case.

As previously noted, the STUDY VESSEL has 27 cargo tanks. Of these, 13 normally carry petroleum products; these are always some form of fuel, such as automotive or aircraft gasolines of all commercial grades, jet fuels or heating oils. Four of the tanks carry lubes of various grades. The remainder are used for a large variety of solvents and other chemicals. Nearly all of these cargoes can form vapors falling in the explosive range under temperature conditions in which the ship operates. The logic diagram was developed to apply singly to any one of these cargo tanks. If a quantitative solution to the diagram were possible, the probability calculated

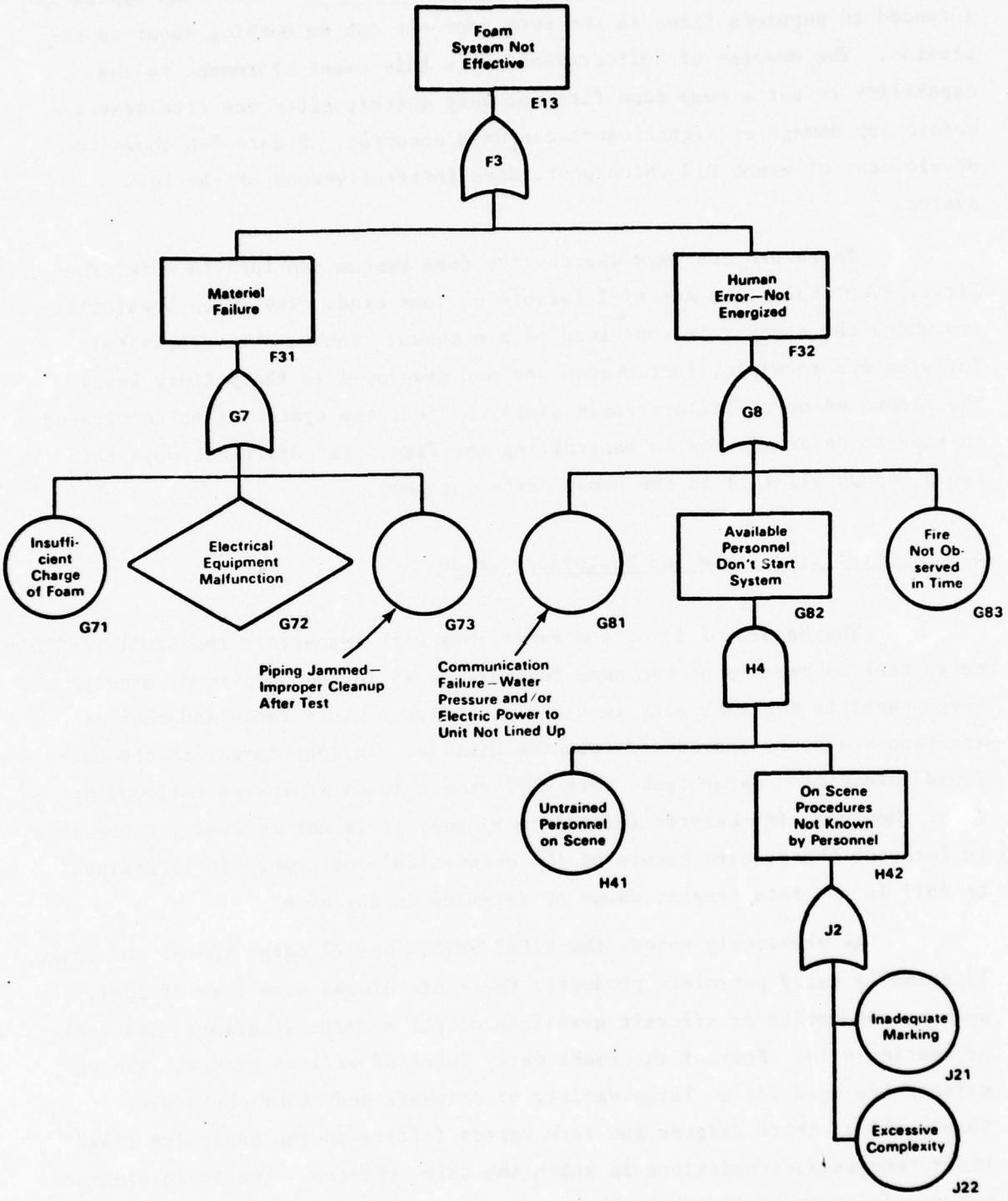


FIGURE 4-6. EVENT E13 DEVELOPMENT--"FOAM SYSTEM NOT EFFECTIVE"

for the top event "Fire or Explosion in a Cargo Tank" would apply to some one tank selected for analysis. To get the probability of a fire or explosion in any cargo tank, one would have to sum the probabilities for all the individual tanks. Since a qualitative solution is being sought in this study, the focusing of the analysis at the level of an individual tank is considered satisfactory for purposes of hazard identification and description.

In this analysis, the cargo tank hazards were studied as they pertained to each of four operating conditions of the vessel.

- Transferring cargo to or from the ship while tied up at the dock (Phases 1 and 2)
- The southbound trip when the ship is underway, unloaded, at sea with cargo tank cleaning/preparation operations being conducted (Phase 9)
- Cruising, loaded on the northbound trip (Phases 3, 5, and 6)
- Underway, unloaded and in ballast (Phases 4, 7, and 8).

This division was found necessary because the sets of circumstances having the potential to cause fires or explosions in the tanks differ among these operating conditions. In the design of the logic diagrams, the different conditions are defined for the branches where they apply by the use of the "house" symbol (see definition in Appendix D). This symbol is combined with the other events of the branch under an AND gate. The event described in this symbol is a routine aspect of the operating phase involved; hence, its probability is essentially unity when the phase is being conducted and zero when it is not. With these values, the event acts as a mathematical switch turning the branch "on" for the operating phase involved and "off" for all other phases.

This organization of the cargo tank diagram is presented in Figure 4-7 along with a full development of the "During Cargo Transfer" branch. This development, and the three others, are discussed in the following subsections.

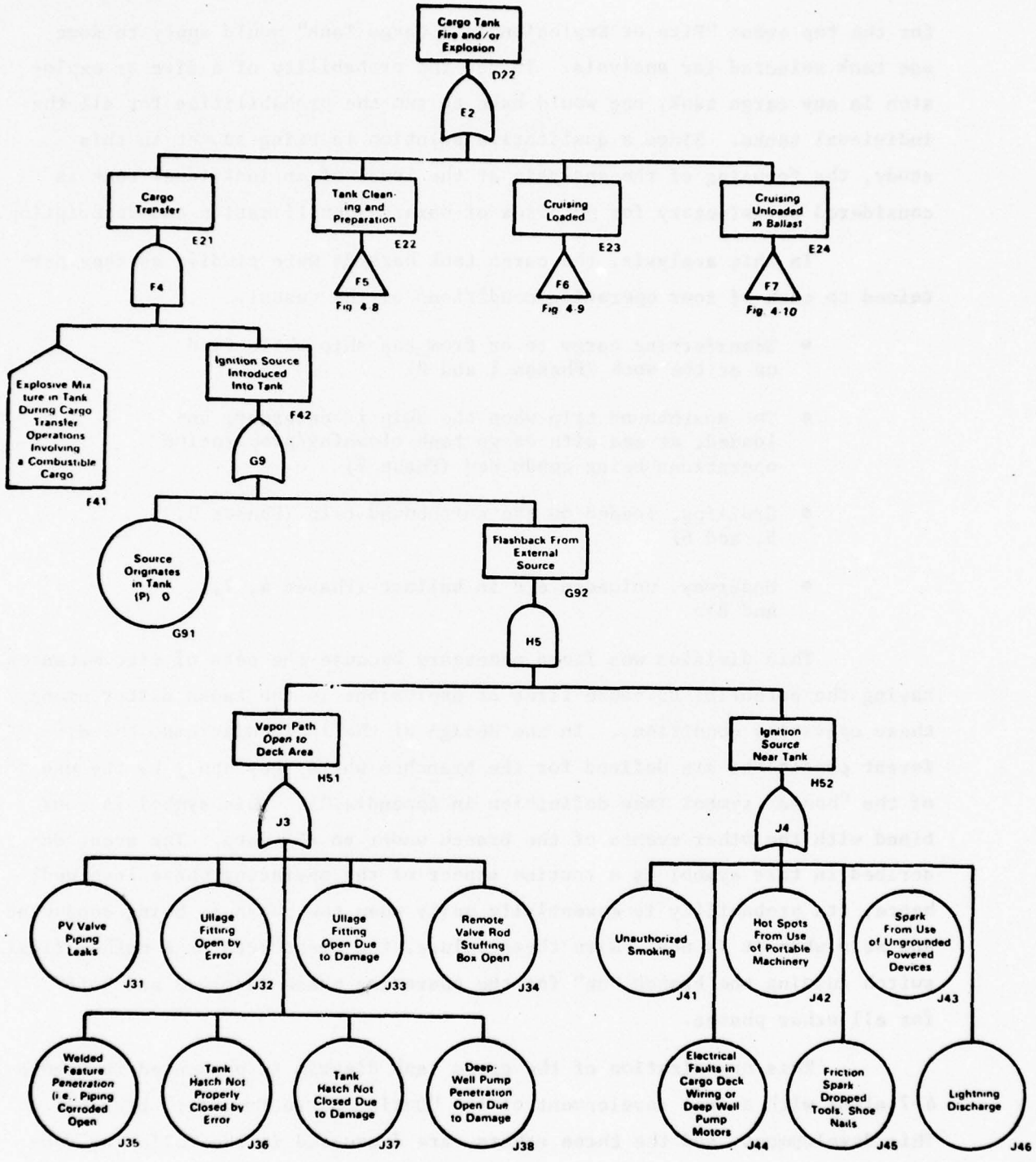


FIGURE 4-7. EVENT PATH D22-E21 DEVELOPMENT--"CARGO TANK FIRE A/O EXPLOSION DURING CARGO TRANSFER"

4.3.2.1 Event E21, Cargo Tank Fire or Explosion During Cargo Transfer. The E-level of the diagram indicates the four operating conditions to be developed in this portion. The detailed development of the E21 branch begins at that level with the expected presence of an explosive mixture in the tank combined with an ignition source. The diagram notation implies that there will always be an explosive mixture present in the tank when any combustible material is being loaded or unloaded. This is not strictly true--in some cases, the properties of a particular cargo and the temperature conditions under which it is being transferred may maintain the tank in the over-rich or under-rich conditions. For purposes of safety analysis, however, it is wise to assume an explosive mixture is always present during this operation.

The diagram is then developed to show the ways by which an ignition could occur. At the G-level, two conditions for this are named but one is rejected at sight since the investigating team could think of no way by which an ignition source could originate inside the tank during cargo transfer (this is the reason for the notation on that event that its probability is essentially zero). Several means were conceived by which a flashback into a tank could occur. In event H51, it is noteworthy that the intended meaning of an "open" vapor path is that it is a continuous path for vapor from the tank to the open deck area without an effective flame arrest device to cut off a flame front trying to propogate into the tank. In considering the different ignition source possibilities (the J4x event group), note that the probability of the behavioral items (such as J41, unauthorized smoking) is very small since special vigilance is observed by the watchstanders on the STUDY VESSEL to see to it that safety precautions and good practices are observed by all hands during loading or unloading. For example, during the first night of the observation cruise while the ship was completing discharge of cargo, all operations were stopped when an electrical storm came up. Smoking discipline appeared to be excellent. This is in line with a basic approach to fire safety during cargo transfer--prevent the ignition from taking place since vapor, probably in the explosive range, is likely to be present for one reason or another during these operations.

4.3.2.2 Event E22, Cargo Tank Fire and Explosion During Tank Cleaning and Preparation. The tank cleaning and preparation phase extends from the initial action of hose washdown from above through machine washing, gas freeing, and, finally, entry in the tank of working parties for final cleaning and drying if circumstances indicate the need. All of these operations are routinely performed on the STUDY VESSEL. Each of these aspects of the cleaning/preparation operation is attended by hazards.

The diagram showing these hazards is in Figure 4-8. The upper level portrays the basic circumstance of an ignition source coming into the tank when an explosive mixture is present. Again, it is not strictly the case that an explosive mixture is inevitably present but the condition is postulated for the purposes of safety analysis. Note that two of the events on this diagram, K11 and J71, are developed the same as event H52 (Figure 4-7) as indicated by the transfer symbols.

4.3.2.3 Event E23, Cargo Tank Fire and Explosion During Cruising Loaded. In this part of the diagram (Figure 4-9) the presence of an explosive mix ure in the ullage space is postulated. This is a rare condition; in most cases, the ullage space would be filled with an over-rich mixture and no combustion could occur. However, the occurrence was judged to be conceivable and was therefore retained. The different modes by which an ignition could occur are identical to those under event F42; this is recognized in this diagram by the transfer symbol attached to event F63.

4.3.2.4 Cargo Tank Fire and Explosion During Cruising, Unloaded and In Ballast. The implicit assumption in this portion of the diagram (Figure 4-10) is that the tank of interest is one of the STUDY VESSEL's center tanks that normally carry high purity chemicals. These tanks are never used for ballast. Frequently, because of changes in the loading schedule at the southern terminal, they require very thorough cleaning after which they are closed up for the remainder of the southbound voyage. It is this closed and empty condition that is the subject of the diagram. The casualty envisioned is that an explosive mixture builds up in the empty tank due to leakage from adjacent spaces or the product piping system and is

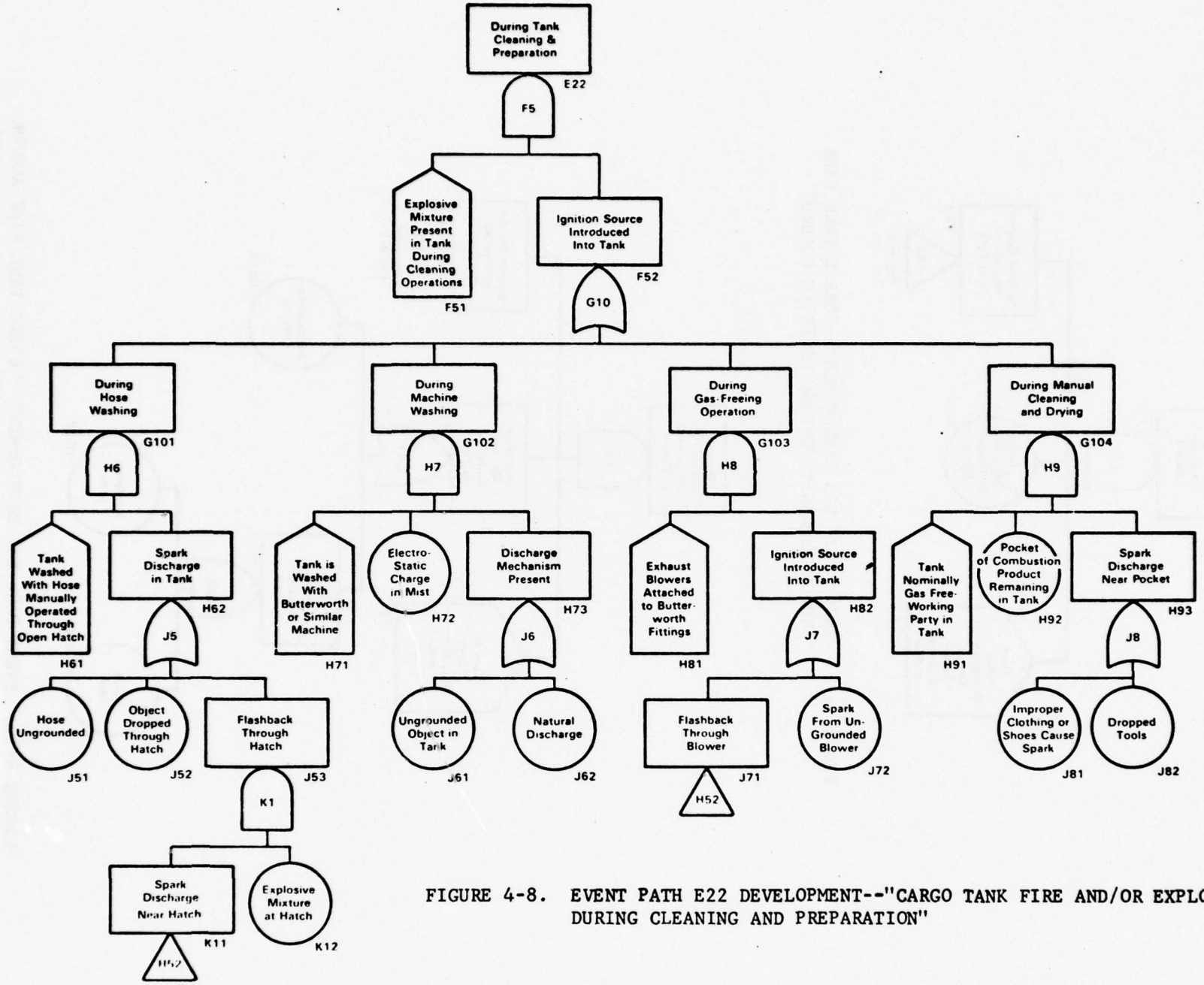


FIGURE 4-8. EVENT PATH E22 DEVELOPMENT--"CARGO TANK FIRE AND/OR EXPLOSION DURING CLEANING AND PREPARATION"

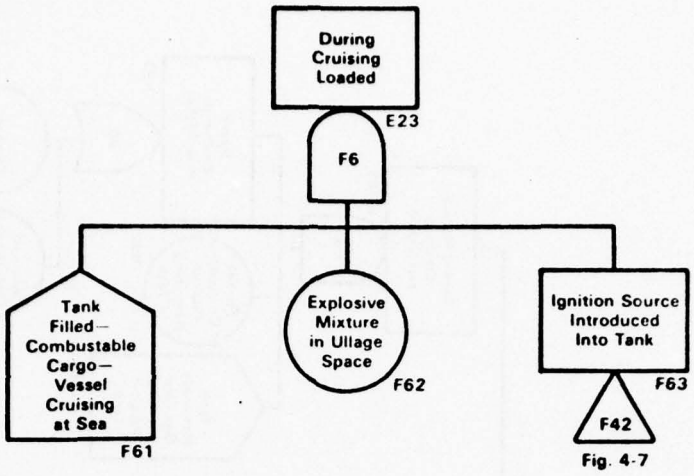


FIGURE 4-9. EVENT PATH E23 DEVELOPMENT--"CARGO TANK FIRE AND/OR EXPLOSION DURING CRUISING LOADED"

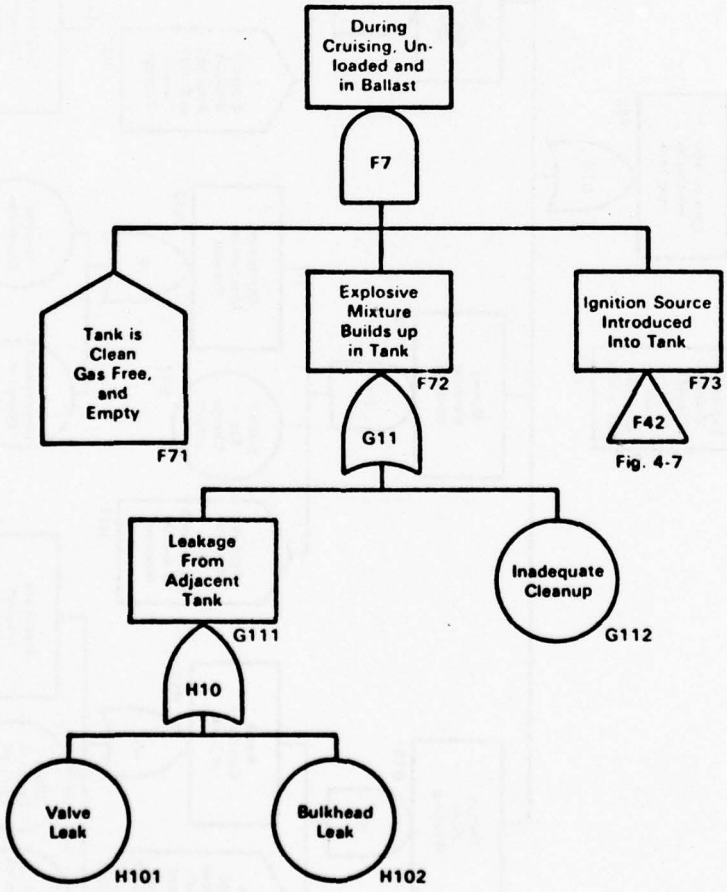


FIGURE 4-10. EVENT PATH E24 DEVELOPMENT--"CARGO TANK FIRE AND/OR EXPLOSION DURING CRUISING UNLOADED AND IN BALLAST

ignited by flashback. As indicated on the diagram by the transfer symbol, the flashback events are the same as event F52 portrayed in Figure 4-7. The former event, leakage, is of extremely low probability in the case of the STUDY VESSEL because her southbound voyage is normally done with no cargoes aboard at all, only ballast, so there would be no combustible material to leak in. However, she does occasionally discharge one or two parcels at a second terminal during the southbound voyage. In any case, it was decided, the possibility of leakage into an empty cargo tank should be documented in this diagram.

4.3.3 Topside Area Fire and Explosion Study

Hazards potentially leading to cargo fires on the STUDY VESSEL's topside are depicted in the diagram of Figure 4-11. The accident is visualized as resulting from the simultaneous occurrence of three events. First, a substantial spill of cargo onto the main deck or other topside area occurs. Second, the spill is ignited. Third, the means at hand for quickly extinguishing the blaze prove to be ineffective so the fire is able to burn a significant length of time--long enough to damage the vessel and hazard the crew. The diagram shows these events as three branches proceeding from the top accident statement through an AND gate.

The "spill occurs" branch, event E31, shows three general ways by which cargo might be released to the main deck area. The first, pipeline leakage, is a primary failure event avoidable through proper maintenance of topside piping. The second is a failure in the cargo transfer system, event F82; it can occur only during transfer operations as indicated by the "housed" structure in the branch. The basic failures underlying this event are either ruptures or overflows--mainly personnel errors. The third spill producing event, F83, is a vessel casualty in which cargo tanks are ruptured as a secondary consequence of a collision, a ramming, or other vessel casualty. This event is not developed in further detail in this analysis since it is outside the cargo system scope of this study.

The "ignition" branch consists of that single event, E32, depicted as a primary failure and not developed in further detail. It was decided to

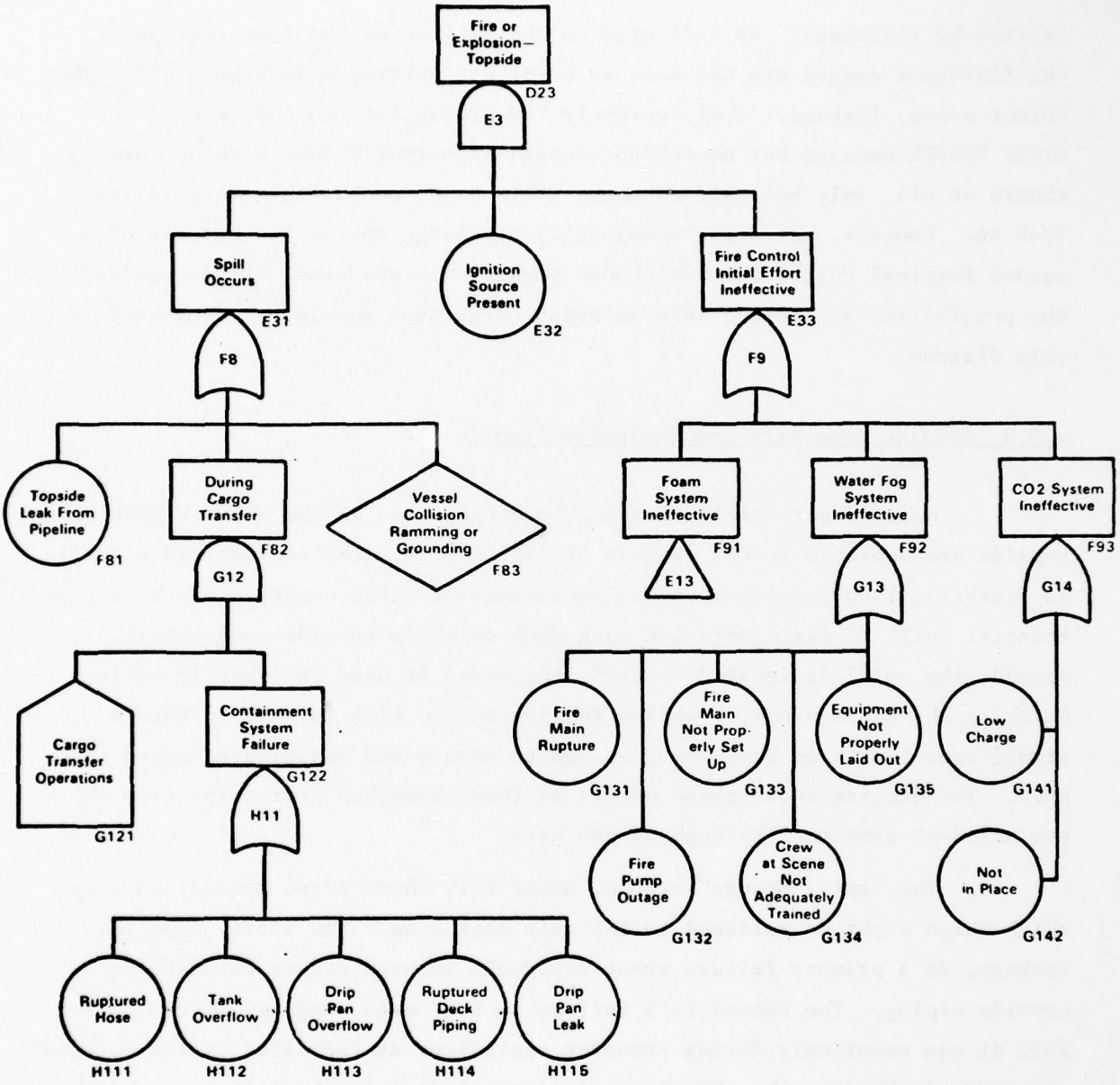


FIGURE 4-11. EVENT PATH D23 DEVELOPMENT--"FIRE OR EXPLOSION IN TOPSIDE AREA"

portray the branch in this way because the probability of an ignition given a spill of any significance is high and, for qualitative safety analysis purposes, has been assumed to be unity. This is an arbitrarily conservative assumption since it puts the full responsibility for controlling this accident on spill avoidance and fire fighting means and gives no credit to the measures taken aboard the STUDY VESSEL to suppress ignition sources on the topside area. The assumption is not intended to denigrate the importance of these measures in any degree or to refute the basic approach to fire safety during cargo transfer operations alluded to in Section 4.3.2.1. It merely accounts for the fact that the vapor cloud formed when a topside spill occurs is not confinable or controllable in any way and will tend to seek out any ignition opportunities that may exist in the area in spite of the best efforts made to eliminate them.

The structure of the third branch developed out of event E33 is based on the doctrine aboard the STUDY VESSEL that the primary means of fighting topside cargo fires is the fixed foam system. The foam system would, of course, be complemented by use of water fog and CO_2 in accordance with standard procedures for fighting Class B fires. However, these latter two also comprise the backup system for fighting the fire if, for some reason, the foam system is inoperative or delayed in being brought into action. The branch is built under an OR gate meaning that the failure of any one of the three systems renders the fire fighting effort ineffective. The "foam system ineffective" branch has already been developed as event E13 in Figure 4-6.

4.3.4 Fire and Explosion Hazard Analysis

The purpose of hazard analysis in the context of system safety practice is to assess the criticality of the hazards that have been identified. In this study, the basic events, depicted on the logic diagrams as circles, constitute the inventory of identified hazards. Each of these hypothesized events fits the classic definition of what a system hazard is, i.e., a condition that exists or could occur in the system having the potential to cause an accident. In this case, of course, this inventory of hazards has to do with only one type of accident, fire or explosion in the STUDY VESSEL's cargo system.

The criticality of a hazard, in this study, is measured by the relative importance of carrying out an act of inspection aimed at subduing or eliminating the hazard. Those hazards found to be of the greatest importance by this measure would be in the top category of the SCP, and the corresponding inspections would have first priority on the inspector's time and resources. A method of assessing criticality in these terms had to be developed.

Ordinarily, in system safety analysis activities, hazard criticality is closely related to the idea of risk where risk is thought of as the product of the probability of a particular accident and its cost. This product is the expected loss in a given length of time due to the occurrence of the accident. The higher the expected loss or risk the more critical the hazard and the more important it is to control it if possible. Thus the control of a hazard may be thought of as a benefit whose value is the change in risk (reduction of expected loss) accomplished.

It was decided that the most useful measure of hazard criticality was the benefit to be obtained in terms of risk reduction by inspecting and correcting the conditions giving rise to that hazard. Accordingly, an assessment procedure was developed to measure this benefit for each hazard. In developing the procedure, the project team recognized at the outset that it would have to be a qualitative one since probability data on the basic events in the logic diagram are virtually non-existent. Qualitative methods of assessment involve the placing of items in arbitrarily defined categories with respect to the various elements of criteria involved; no deterministic calculations can be made to facilitate such categorization. It is essential that such an assessment methodology be kept as simple as possible. Since arbitrary judgements are involved, the more complex the method the greater are the opportunities presented for plausible but arbitrary manipulation of the results and the less credibility is likely to be attached to them. Simplicity in such methodologies is achieved in two ways:

1. Keep the number of criteria elements to be applied and integrated to a minimum.
2. Define the categories into which the evaluative items are to be placed in physical or phenonenological terms as much as possible so the choices are stark and well-defined.

The methodology developed for this criticality evaluation involved judging each of the hazards as to its "inspectability" and then categorizing the inspectable hazards as to three criteria: (1) accident severity, (2) impact of the inspection process on the liklihood of the basic event, and (3) the number of events in the accident path.

4.3.4.1 Inspectability. Many of the basic events in the logic diagrams are not inspectable for one reason or another, that is, the conditions which would have to exist to cause the event are either not detectable by inspection or inspection has no power to reduce the probability of the event's occurring in the future (or both). An example is the event of a cargo pump overheating through being allowed to lose suction and run vapor-bound so as to become a possible ignition source. A Coast Guard inspector conducting a regular inspection of a vessel has no way of detecting the possible future occurrance of that condition--it is purely a function of correct machinery operating procedure on the part of the crew. The risk involved with such events can't be affected by inspection hence no benefit is possible. Thus, hazards categorized as not inspectable were dropped from this evaluation process. This does not mean that such hazards are unimportant. Indeed, many hazards that can't be inspected for are more significant to the vessel's safety than the ones that can be. It merely means that uninspectable hazards are not relevant to this particular study.

4.3.4.2 Accident Severity. Accidents do not have equal severity. As was discussed in connection with the PHA (Section 4.2.1.5), the damage and loss expectation is more severe with some accidents than others. Hazards leading to the more severe accidents were judged to be correspondingly more critical, all other things being equal.

In formulating this criterion for use in assessing the logic diagram hazards, the same scheme of categorization shown in Table 4-1 was employed except that some simplification proved to be both possible and necessary. In that table, categories III and IV were subdivided by party-at-risk exposure levels. These subdivisions relate directly to where the vessel is when she experiences an accident. If she has an explosion at sea where only the vessel and crew are at hazard, the accident is categorized as IV A. If the same accident occurs while the ship is tied at the dock in a populous port the public and public property are also hazarded along with the close in marine environment. In this case the hazard category is IV C,

two levels more severe than in the former case.

This fine-graining of the hazard categories was necessary in conducting the PHA where one of the purposes was to spot the high-risk portions of the vessel's operating cycle. However, in the case of the present assessment, these operating cycle differences have no meaning. An act of inspection aimed at preventing a certain type of explosion, if successful, will prevent it for a year or more during which time the ship passes through all possible operating phases many times. The criticality of the explosion relative to the inspection act preventing it is insensitive to operational phase and the parties-at-risk variations involved. Accordingly, only the 4-part base categorization scheme which describes the inherent severity or violence of the accident regardless of location was used in this assessment. Furthermore, category I, negligible, was dropped leaving three levels of severity to be considered.

4.3.4.3 Event Probability Impact. The fundamental purpose of conducting an act of inspection is to alter the probability of occurrence of the failure event involved. If an inspector discovers excess plate wastage in a vessel's hull it can be interpreted as meaning the probability of structural failure in the near future (within the time of the oncoming inspection interval) is unacceptably high. If he requires that the condition be corrected by installing new plating (restoring the vessel structure to design strength conditions) then the probability of the failure has been greatly reduced, indeed, it has been made essentially zero for the ensuing inspection interval. This, of course, constitutes a major impact on that event's probability. Making such an impact is really the only way the inspection process can produce benefits of the kind discussed earlier in section 4.3.4. The criterion applied here, then, is the relative magnitude of this benefit that can be obtained by a given act of inspection related to a given hazard.

To assess this with respect to a given hazard, it was necessary to develop a qualitatively defined set of impact categories into which the hazard can be fitted by considering the nature of the indicated inspection procedure and the mode of degradation leading to the occurrence of the event. Three descriptors of such categories were developed.

- Maximum impact. The greatest impact on event failure probability results when the probability of the event without inspection is essentially one and the act of inspection changes the probability to essentially zero for the period of the ensuing inspection interval. This occurs when the failure event is brought about through the action of a time-stress function such as atmospheric corrosion (probability of one if the degradation process is not interrupted), and the inspection process is capable of detecting the condition accurately and requiring full restoration to the design condition by a means that is permanent and intrinsic in the material makeup of the vessel. An obvious example of this kind of impact is the one mentioned above where wasted plating is replaced. The "fix" is a permanent part of the structure of the ship and is not dependent in any way on the crew's observing correct operating procedures, avoiding of human error, or the like. The inspection process exerts full control over the hazard independently of any other agencies or actors.

- Moderate impact. Inspection can effect a moderate reduction of the probability of a failure event where the failure will result from improper maintainence or operation that has already caused a detectable amount of degradation. The inspector can require that the observed condition be rectified and in so doing can exert pressure on the ship's officers and crew to carry out proper procedures. An example of this type of condition would be the discovery of CO_2 extinguishers not properly charged, excessive product drippings in the pump room bilges, or cargo tank wash hose with inadequate provisions for grounding. The inspection process can detect many such conditions where they show up as material defects. However, the inspection process does not have full control of these hazards since this will depend on the crew's using correct operating procedures in the future.

- Minimal impact. The inspection process can expect to have only small impact on the probability of a failure event whose probability is logically small to begin with. A failure resulting from an error in the original construction of the ship, for example, would be of low probability because the condition had already been checked for at the time of construction. Thus, it is unlikely that an inspector working on a ship that has been in operation for some time would find the safety lamps in the pump room lower level to be improperly installed. In addition, hazards were placed in this impact category when there was a serious question as to whether or not the condition could be detected by inspection. The sudden failure of a cargo transfer hose because of fatique of internal parts might fall in this category.

4.3.4.4 Number of Events in Accident Path. The number of failure event paths involved in any given accident can be readily determined by inspection of the logic diagram depicting it. An accident that can be caused by a single failure event is more probable than one that can result only if two or three independent failure events occur simultaneously. It follows from this that failures in a single event path are more critical than those in multiple event paths. It is this, incidently, that leads to the safety engineer's rule of thumb that relatively dangerous situations are represented by logic diagrams having OR gates high in the structure, whereas relatively safe situations exist when there are AND gates there. In the present study, the pump room and topside logic diagrams depict three-event accidents whereas the cargo tank diagram involves a single-event accident. Because of this the basic events in the first two diagrams are of relatively lower criticality than the ones in the latter.

4.3.4.5 Integration of Criteria. For each hazard, the criteria levels were combined directly and the hazard was then located as to criticality in a grouped rank-ordering. The most critical hazard would be one capable of triggering a category IV accident by itself due to progressive corrosion of some vital part of the ship. The next lower level of criticality would be assigned that hazard if it was in one lower category with respect to any one of the three criteria discussed above. As a matter of convenience in keeping track of the evaluations for each hazard, numerical values were assigned to all the criteria levels, the most critical being represented by one and the least by three. The example mentioned above would have a one for each category giving an integrated number of three. These numbers have no significance except as they act as surrogates for the names of assessment categories.

Table 4-2 indicates the criticality ranking values chosen for the SCP and the assessment combinations falling in each one. Three ranking levels were selected.

- Mandatory--indicated inspection item is important enough that it must always be inspected.
- Critical--indicated inspection item is of intermediate level importance mainly because hazard is less subject to control through the inspection process.

TABLE 4-2. CRITICALITY ASSESSMENT COMBINATIONS

SCP Ranking	Criteria Level Combinations
Manditory	Numerical combinations summing to 4 or less
Critical	Numerical combinations summing to 5
Routine	Numerical combinations summing to 6 or greater

- Routine--inspect on a routine basis but no priority is attached either because the hazard involved is of lower severity or because the inspection process exerts little control over the hazard.

More levels with a finer-grained variation among them could have been defined for this evaluation. However, this would have had little practical meaning for the inspection process; it will be difficult enough for an inspector to recognize two levels of prioritization beyond routine, let alone three or more.

The numerical assessment combinations shown in Table 4-2 were arbitrarily chosen after the hazards discovered in this study had been tabulated in order of relative importance. These break points for the different levels yield a satisfactory distribution and reflect significant steps in the three "importance criteria".

4.3.4.6 Assessment of Hazards. Table 4-3 shows the criteria assessments and criticality class assignments made for each of the basic events in the fire or explosion diagrams for the pump room, cargo tanks, and topside areas. The first column shows a brief description of the inspection action deemed appropriate for each hazard listed. The remaining columns show criteria evaluations and class assignments.

TABLE 4-3. HAZARD CRITICALITY ASSESSMENT

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
H11.	Pump room vent motor electrical malfunction	Inspect (megger and visual) for insulation deterioration or other conditions leading to spark generation	1	1	3	Critical
H12.	Electrostatic discharge in pump room exhaust duct	Visual inspection for degraded conditions in duct work (corrosion, cracking) leading to the presence of loose metallic objects in the exhaust ducting	1	1	3	Critical
H13.	Friction spark in pump room exhaust duct--foreign or loose object	Ditto	1	1	3	Critical
G21.	Broken lamp cover in pump room	Visual	1	1	3	Critical
G22.	Incorrectly installed lamp cover	Ditto	1	3	3	Routine
G31.	Vapor bound cargo pump	Not inspectable--specific operational conditions	--	--	--	--
G32.	Tight packing in cargo pump	Operational check	1	2	3	Routine
G33.	Cargo pump bearing overheated	Operational check	1	2	3	Routine
G34.	Hot lamp cover	Visual and touch	1	1	3	Critical
G41.	Dropped tools in pump room area	Not inspectable--operating procedure	--	--	--	--
G42.	Nails in shoes worn by men entering pump room	Ditto	--	--	--	--
G43.	Inadequately sealed flashlights carried by men entering pump room	"	--	--	--	--

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
G44.	Ungrounded power tools in use in pump room	Uninspectable--operating procedure	--	--	--	--
G45.	Improperly stowed items in pump room come adrift and drop	Check for improper use of pump room as a stowage area	1	3	3	Routine
F15.	Unauthorized smoking in pump room	Essentially uninspectable. Observe discipline of vessel crew--visually check "no smoking" signage aboard vessel	--	--	--	--
F21.	Large containment failure in pump room	Inspect for wastage in piping, fittings, and tank structure in pump room and contiguous spaces	1	1	3	Critical
G51.	Cargo pump packing failure	Operational inspection plus maintenance check	1	2	3	Routine
G52.	Pinhole in pressure system part (pump room)	Inspect piping and fittings including gage lines and other small, pressurized systems	1	2	3	Routine
H21.	Human error--vent system not turned on	Not inspectable--operating procedure	--	--	--	--
H31.	Drip/drain accumulation of product in pump room bilges	Inspect for actual accumulation or evidence of past accumulations	1	2	3	Routine
H32.	Small containment failure	Inspect for small leaks	1	2	3	Routine
J11.	Pump room exhaust vent motor failure	Operational and visual check of feeder, controller and motor	1	1	3	Critical

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
J12.	Pump room exhaust vent ducting failure causing short circuit	Inspect for wastage in all parts of the ducting system	1	1	3	Critical
G71.	Insufficient charge of foam in fixed foam generator	Operational check of foam generator	1	1	3	Critical
G72.	Electrical equipment malfunction	Operational inspection of foam system plus inspection of feeders and controllers with megger test of system	1	1	3	Critical
G73.	Foam generator piping jammed due to improper cleanup after test	Inspect for proper cleanup after test	1	1	3	Critical
G81.	Communication failure--water pressure and/or electric power to foam generator not properly lined up	Uninspectable--operational procedure	--	--	--	--
G83.	Fire not observed in time	Not inspectable--human performance	--	--	--	--
H41.	Untrained personnel on scene	Not inspectable--function of training program	--	--	--	--
J21.	Inadequate marking (of piping and controls of the fixed foam system)	Visual inspection	1	1	3	Critical

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
J22.	Excessive complexity (of procedures to activate foam system)	Not inspectable--function of design and state of training	--	--	--	--
G91.	Ignition source originates inside cargo tank during cargo transfer operations--probability approximately 0	No inspection procedure definable	--	--	--	--
J31.	PV valve piping leaks	Inspect piping for material condition and incipient failure	1	1	2	Mandatory
J32.	Ullage fitting open by error	Not inspectable--human performance	--	--	--	--
J33.	Ullage fitting open due to damages	Inspect ullage fittings	1	2	2	Critical
J34.	Remote valve operator stuffing box open	Inspect stuffing boxes	1	2	2	Critical
J35.	Welded feature penetration (i.e., piping) wasted to open condition	Inspect for wastage	1	1	2	Mandatory
J36.	Tank hatch not properly closed due to error	Not inspectable--human performance	--	--	--	--
J37.	Tank hatch not properly closed due to damage	Inspect hatches and check function	1	2	2	Critical
J38.	Deepwell pump penetration open due to damage	Inspect all penetrations	1	1	2	Mandatory
J41.	Unauthorized smoking on main deck	Not inspectable--function of training, indoctrination, and discipline	--	--	--	--

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
J42.	Hotspots from use of portable machinery	Not inspectable--operating procedure	--	--	--	--
J43.	Spark from use of ungrounded powered devices	Ditto	--	--	--	--
J44.	Electrical faults in cargo deck wiring or deepwell pump motors	Inspect and megger circuits/equipment	1	2	2	Critical
J45.	Friction spark from dropped tools, nails in shoes, etc.	Not inspectable--operating procedure	--	--	--	--
J46.	Lightening discharge	Ditto	--	--	--	--
J51.	Tank wash hose ungrounded	Check hose for proper grounding provisions	1	2	2	Critical
J52.	Object dropped through hatch	Not inspectable--operating procedures--state of training	--	--	--	--
K12.	Explosive mixture at hatch	Not inspectable--transient operational condition	--	--	--	--
H62.	Electrostatic charge in mist (during machine washing of tanks)	Ditto	--	--	--	--
J61.	Ungrounded object in tank (during machine washing)	Not inspectable--operating condition	--	--	--	--
J62.	Natural discharge in tank (during machine washing)	Ditto	--	--	--	--
J72.	Spark from ungrounded blower (during gas freeing)	"	--	--	--	--

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

	Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
H 2.	Pocket of combustible product remaining in tank	Not inspectable--operational procedure	--	--	--	--
J81.	Improper clothing or shoes cause spark (during manual tank cleaning)	Ditto	--	--	--	--
J82.	Dropped tools	Not inspectable--operational/behaviorial factors	--	--	--	--
F62.	Explosive mixture in ullage space	Not inspectable--operational condition	--	--	--	--
G112.	Inadequate tank cleanup (during cruising unloaded)	Not inspectable--operational procedure	--	--	--	--
H101.	Valve leak	Inspect tank lines for evidence of leakage	1	2	2	Critical
H102.	Tank bulkhead leak	Inspect tank structure for cracks, wastage, evidence of incipient failure	1	1	2	Mandatory
F81.	Leak in cargo deck piping	Inspect for wastage and evidence of leaks	1	1	2	Mandatory
H111.	Hose rupture (during cargo transfer operations)	Inspect vessel hose plus check of dockside hose.	1	3	3	Routine
H112.	Tank overflow	Not inspectable--operational procedure	--	--	--	--
H113.	Drip pan overflow	Ditto	--	--	--	--
H114.	Ruptured deck piping	Inspect for wastage and evidence of incipient failure under pressure	1	3	3	Routine
H115.	Drip pan leakage	Inspect drip pans	1	1	3	Critical

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

TABLE 4-3. (Continued)

Basic Event	Inspection Action	Accident Severity[a]	Event Probability Impact[b]	No. of Parallel Events in Accident Path[c]	SCP Classification
G131. Fire main rupture	Operational/visual inspection of fire main piping and fittings	1	1	3	Critical
G132. Fire pump failure	Operational/visual inspection of pump, motor, controller plus megger test	1	1	3	Critical
G133. Fire main not properly lined up	Not inspectable--operational procedure	--	--	--	--
G134. Inadequate training of crew at hand	Not inspectable--training/awareness level	--	--	--	--
G135. Equipment not properly laid out (fog nozzles, hose, etc.)	Not inspectable--operating procedure	--	--	--	--
G141. Depleted charge (CO_2 equipment)	Check charge level during inspection	1	2	3	Routine
G142. Equipment not in place (CO_2 portable equipment	Not inspectable--operating	--	--	--	--

(a) 1 - catastrophic, 2 - critical, 3 - negligible.
(b) 1 - maximum impact, 2 - moderate impact, 3 - minimal impact.
(c) 1 - single-event path, 2 - two-event path, 3 - three or more event path.

The SCP extracted from this analysis is portrayed in Figure 4-12. It is arranged as a screen format to illustrate how the SCP might be presented to a user of VIIS. In constructing this figure, the items from Table 4-3 falling in the "mandatory" and "critical" categories were grouped into logical inspection items wherever such grouping was possible. For example, Items G12, G13, and J12 in the "critical" class all are concerned with failures occurring in the pump room exhaust vent system. They were regrouped as shown for inclusion in the SCP. In addition, each item was restated so as to specify the type of degradation to be inspected for (the "inspection" column) and the failure to be controlled by the inspection.

DATE/ _____ VESSEL SAFETY CRITICAL PROFILE PAGE 1 OF 2

ITEM	INSPECTION	HAZARD
	A. MANDATORY INSPECTION ITEMS	
CARGO TANK VENT PIPING	FUNCTION AND MAT COND	OPENINGS INTO TANKS
MAIN CARGO DECK	WASTAGE--PLATING/WELDED FEAT	OPENINGS INTO TANKS
CARGE TANK BULKHEADS	MAT COND RE WASTAGE/CRACKS	NEXT SPACE LEAKAGE
MAIN DECK CARGO PIPING	MAT COND RE WASTAGE/CRACKS	LEAKS TO TOPSIDE AREA
	B. CRITICAL INSPECTION ITEMS	
PUMP RM EXH VENT MOTOR	MECH COND--ELECT INSULATION	SPARK DISCHARGE
PUMP RM EXH VENT TRUNK	MAT COND--WASTAGE/LOOSE OBJ	AIR LEAK--SPARK DISCHARG
PUMP RM LIGHTING	INSTALLATN--BREAKAGE--HOT	HOT SPOT IGNITION SOURCE
PUMP RM PIPING/STRUCT	MAT COND--WASTAGE/CRACKS	INCIPIENT LEAKS
F/FOAM GENERATOR	ADEQUATE FOAM CHARGE	INOPERABLE IN EMERGENCY
--ELECTRICAL EQUIPMENT	FUNCTION--INSULATN--MAT COND	EMERGENCY SERV FAILURE
--PIPING	FUNCTION--FREE OF STOPPAGE	INOPERABLE IN EMERGENCY
--OP INST & MARKINGS	ADEQUATELY PRESENT	INOPERABLE BY PERSONNEL
CARGO TANK ULLAGE FTGS	DAMAGE OR WASTAGE	NONCLOSURE OF TANK
REM VALVE STUFF BOXES	MAT COND--TIGHTNESS	NONCLOSURE OF TANK
CARGO TANK HATCHES	MAT COND--DAMAGE	NONCLOSURE OF TANK
CARGO TANK WIRING	MAT COND--INSULATION	SHORTING--SPARK DISCH

COMMAND/_____ RESPONSE/_____

FIGURE 4-12. SAFETY CRITICAL PROFILE

DATE/ _____ VESSEL SAFETY CRITICAL PROFILE PAGE 1 OF 2

ITEM	INSPECTION	HAZARD
	B. CRITICAL INSPECTION ITEMS (CONT)	
TANK WASH HOSE	ADEQUATE GROUNDING	SPARK DISCHARGE
DRIP PANS	MAT COND--LEAKAGE	LEAKS TO TOPSIDE AREA
FIRE MAIN	MAT COND--OPERATION	EMERGENCY SERV FAILURE
FIRE PUMP	FUNCTION--INSULATN--MAT COND	EMERGENCY SERV FAILURE
CARGO TANK PIPING/VALVS	MAT COND--LEAKAGE	LEAK INTO CARGO TANK

COMMAND/_____ RESPONSE/_____

FIGURE 4-12. (Continued)

4.4 HAZARD MODE AND EFFECT ANALYSIS

The HMEA carried out in this study had the same purpose as the logic diagram analysis just presented, namely, to identify hazards of fire or explosion in the STUDY VESSEL's cargo system and to assess those hazards as to inspection criticality. The HMEA technique involves approaching this task at the component or subsystem level. One lists all the components and subsystems comprising the system of interest, postulates hazardous failures that might occur in each, and then traces the effects of each such failure through the system to determine what type and severity of accidents might result from the failure. Criticality assessment of each hazardous failure possibility is then made on the basis of the evidence thus assembled.

The HMEA process is not conducted in a framework of mathematical rigor; rather, it is highly descriptive in nature and gives the analyst somewhat more freedom to exercise judgment as he proceeds through the various steps. Also, the tabular format on which the analysis is recorded is not rigidly prescribed. The analyst is free to decide what evidence about failures is required to support the particular decisions he intends to draw out of the HMEA process. The steps carried out in an HMEA, then, are (1) develop the list of components/subsystems comprising the system to be investigated, (2) design an HMEA format suiting the needs of the particular analysis, and (3) carry out the analysis.

4.4.1 Components and Subsystems Analyzed

The STUDY VESSEL's cargo system was briefly described in Section 2.1 and covered in greater detail in the discussion and figures of Appendix A. In preparing to perform this HMEA, it was decided to organize the listing of items to be studied in accordance with the general breakdown listing of vessel systems presented in Appendix B. Figure 4-13 shows the resultant listing tailored to the particular systems and components aboard the STUDY VESSEL.

Level I	Level II	Level III and Listings
9. Cargo System	1. Cargo Environment Control	1. Pressure Control • PV valves • Flame screens • PV valve piping
		2. Temperature Control • Steam heating coils
	2. Containment System	1. Primary Containment • Cargo tank structural envelope--bulkheads • Cargo tank structure--tank top (main deck plating) • Ullage openings/closure fittings • Hatches
	3. Transfer System	1. Cargo Unloading/Loading • Deck piping/valves • Tank piping/valves • Main cargo pumps 2. Pump Room • Pump room piping/valves • Pump room lighting • Pump room exhaust vent system

FIGURE 4-13. COMPONENT/SUBSYSTEM LISTING FOR HMEA

4.4.2 Development of the HMEA Format

A 13-column format was developed for this HMEA. The columns, moving from left to right, form a succession of information citations and intermediate conclusions about the particular failure and its impact on the system. These are used by the analyst in deciding about the inspection criticality of the failure, a decision recorded in the right end column. The basic reasoning behind this decision was identical to that used in assessing failure event criticality in the logic diagram analysis, namely, criticality is a function of three aspects of a failure: (1) severity of the accident threatened, (2) impact of inspection on the probability of the failure, and (3) number of simultaneous events required to cause the accident. The conventions used in entering the columns are described in the following subsections.

4.4.2.1 Column 1, "Hazard Mode". This column identifies the top-level hazard category to which the analysis is intended to pertain.* In the present case, this entry is always "fire or explosion, cargo system" since the study has been scoped to cover only that topic.

4.4.2.2 Column 2, "Item". In this column, the component or subsystem whose potential failures are to be investigated is named.

4.4.2.3 Column 3, "Subsystem". In this column, the name of the vessel subsystem of which the item forms a part is named. The vessel subsystems in this case are indicated by the Level II and Level III nomenclature from Figure 4-13.

---

* It is the presence of this column in the format that makes this analysis a hazard-mode-effect analysis rather than a traditional failure-mode-effect-analysis as practiced by reliability engineers. In fact, an HMEA is an FMEA except that the left hand column restricts the study to only those failures that could bring about the specified hazard. The reliability engineer explores all consequences of a failure that could result in unreliable performance. The safety engineer explores only those that would bring about unsafe system performance.

4.4.2.4 Column 4, "Function". In this column, the item's function is briefly described. If the item has many functions, then it is only necessary to note those which have safety relevance. However, it is sometimes difficult to know in advance which ones are safety relevant and which are not--the conservative analytical approach is to note them all.

4.4.2.5 Column 5, "Failure/Error". In this column, the specific failure or procedural error to be investigated is recorded. If the item has more than one failure mode of concern to the analysis, each is recorded separately since each failure mode starts a separate analysis.

4.4.2.6 Column 6, "Cause". The cause is the failure mechanism--i.e., excess loading condition, corrosion degradation, failure to observe operating procedures--which could bring about the postulated failure. This is a particularly important entry in this analysis because it indicates the "inspectability" of the failure being studied; this quality is one of the final assessment criteria. If there are several possible causes of the failure, all should be recorded.

4.4.2.7 Column 7, "Immediate Effect". This is the condition that results directly from the failure/error being analyzed. In some cases, this may be the accident (hazard mode) noted in column 1; more often, however, it is the creation of a condition that will contribute to causing the accident if other, independent failures or conditions occur simultaneously or sequentially with the one being analyzed.

4.4.2.8 Column 8, "Ultimate Effect". The ultimate effect of the failure/error is the level of injuries and/or damage that might, in worst circumstances, result from the type of accident that might be caused. Typical entries are couched in these terms, i.e., "si/f & mpd (serious injuries and/or fatalities and major property damage) due to fire and explosions in cargo tank. Thus the entry specifies both the type and severity of the accident.

4.4.2.9 Column 9, "Simultaneous Events or Conditions Required". In this column is indicated the events or conditions, if any, that must also occur along with the failure/error being analyzed for the "ultimate effect" entered in column 8 to be realized. Each such event or condition must be entered because the number of them indicates the number of "paths" involved in a logic diagram portrayal of the accident. The more such paths, the lower the liklihood of the "ultimate effect". The number of such paths is one of the criticality criteria just as it was in the logic diagram approach described previously.

4.4.2.10 Column 10, "Hazard Severity Category". This is the first of the three criticality evaluation criteria to be entered in this HMEA. As before, the schedule of severity categories presented in Table 4-1 is used in the simplified form discussed in section 4.3.2.2 for this evaluation. The category to be used is directly reflected in the citation of the "ultimate effects" in column 8.

4.4.2.11 Column 11, "Inspection Impact of Failure/Error Liklihood". In this column, the effectiveness of the inspection function in subduing the probability of the failure under investigation is rated. This is the second of the three criticality criteria. The ranking is made in accordance with the method described in Section 4.3.4.3.

4.4.2.12 Column 12, "Multiple Event Ranking". This is the third of the criticality ranking criteria. It accounts for the effect on the probability of the ultimate accident of the requirement that independent events occur simultaneously in order to trigger the accident. Such accidents are much less probable than single event accidents. The probability reduction is roughly proportional to the number of simultaneous events required so the entry in the column is simply that number.

4.4.2.13 Column 13, "Inspection Criticality Level Assessment". The same conventions were used in making this assessment in the HMEA as were used in making the final assessments for the logic diagram analysis. These conventions are shown in Table 4-2 and are described in Section 4.3.4.5.

4.4.3. Conduct of the HMEA

The HMEA carried out with respect to the STUDY VESSEL's cargo system is shown in Figure 4-14. The components and subsystems included in the analysis are those listed in Figure 4-13. The entries in the columns of the HMEA are in accordance with the conventions discussed in the preceeding subsections. The analysis brings out with reasonably satisfactory emphasis the fact that nearly all the accidents postulated in this study are multiple-event occurrences, this being the nature of fires and explosions. The scenarios described by the horizontal row entries are also well tuned to the inspection orientation of this study.

It is noteworthy that this analysis was not carried to the level of specific, individual parts and components as is normally done with detailed failure mode and effect analyses in reliability engineering. In such analyses, it is routinely necessary to account quantitatively for the performance of every individual part in the system. Instead, because this was a safety analysis, it was found that functional classes of parts and components (i.e., ullage fittings, main deck piping) could be usefully addressed. To discover how relatively critical the inspection of main deck piping would be, for example, it was only necessary to consider the hazards created by leaks or ruptures in that piping subsystem. Consideration of individual runs of piping or particular valves added nothing to the information that could be generated from the analysis. Similarly, it was found that all the tank containment structure could be considered as one element to be analyzed. This collapsing of the thousands of individual parts and components making up the STUDY VESSEL's cargo system into a relatively small number of component classes made it possible to substantially shorten the HMEA over what it would have been if all components had been considered separately. This point of technique should not be applied blindly in the making of HMEA's, however, it was feasible in this case because of the nature of the inspection process which, itself, considers classes of components rather than individual ones in setting inspection priorities.

Also, the HMEA was scoped to consider only the vessel's cargo system components as the entry items in the tabulation. This sharply limits the range of items whose failures are considered. For example, the fire

HAZARD MODE	ITEM IDENTIFICATION		FUNCTION	FAILURE/ERROR MECHANISM		EFFECT		SIMULTANEOUS EVENTS OR CONDITIONS REQUIRED	INSPECTION CRITICALITY EVALUATION			INSPECTION CRITICALITY LEVEL ASSIGNMENT
	ITEM	SUBSYSTEM		F/E	CAUSE	IMMEDIATE	ULTIMATE		HAZARD SEVERITY CATEGORY	INSPECTION IMPACT ON F/E PROB.	MULTIPLE EVENT RANKING	
1	2	3	4	5	6	7	8	9	10	11	12	13
Fire or explosion	PV valves	Cargo environmental control system	• Prevent excessive pressure or vacuum in cargo tank • Discharge vapor at high upward velocity	Stuck closed	• Jammed by foreign object • Service damage • Corrosion	Pressure build-up in cargo tank being filled	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Tank rupture • Ignition source near rupture	IV	Weak	4	Routine
	Flame screens	Cargo environmental control system	• Prevent flame front propagation into tank	Opening in mesh	• Wastage • Damage	Creates barrier-free vapor path to tank interior	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Fitting off or damaged • Ignition source in vicinity	IV	Strong	4	Critical
	PV valve piping	Cargo environmental control system	Carries vapor to elevated release point	Leak in piping run	• Wastage • Damage	Creates barrier-free vapor path to tank interior	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Ignition source in vicinity	IV	Strong	3	Mandatory
	Cargo heating coils	Cargo environmental control system	Convey heating steam (80 psig) to cargo tank	Rupture	• Metal fatigue (vibration) • Wastage	Steam jet in cargo tank creating a charged mist	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Ungrounded conductor in tank • Erroneous energizing of heating system	IV	Weak	4	Routine
	Cargo tank structural envelope--bulkheads	Cargo tanks	Cargo containment	Leakage opening to/from adjacent space	• Wastage • Cracks due to hull stressing	Creates leakage path for cargo into or adjacent space	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture formation in empty tank • Source of ignition introduction	IV	Strong	3	Mandatory
	Cargo tank structural envelope--tank top (main deck plating)	Cargo tanks	• Cargo containment • Provides main deck structure	Leakage opening to top side	Metal wastage--generally in way of welded penetrations or fittings	Creates barrier-free vapor path from top side to tank interior	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Source of ignition in vicinity of leak	IV	Strong	3	Mandatory
	Ullage openings/ closure fittings	Cargo tanks	Provide flame barriered opening for taking ullage measurements	Opened with barrier ineffective	• Damage in service • Wastage • Failure to close properly during use	Creates barrier-free vapor path to tank interior	si/f & mpd due to fire or explosion in cargo tank	• Explosive mixture in tank • Ignition source in vicinity of fitting	IV	Moderate	3	Critical

FIGURE 4-14. HAZARD MODE AND EFFECT ANALYSIS

HAZARD MODE	ITEM IDENTIFICATION		FUNCTION	FAILURE/ERROR MECHANISM		EFFECT		SIMULTANEOUS EVENTS OR CONDITIONS REQUIRED	INSPECTION CRITICALITY EVALUATION			INSPECTION CRITICALITY LEVEL ASSIGNMENT
	ITEM	SUBSYSTEM		F/E	CAUSE	IMMEDIATE	ULTIMATE		HAZARD SEVERITY CATEGORY	INSPECTION IMPACT ON F/E PROB.	MULTIPLE EVENT RANKING	
1	2	3	4	5	6	7	8	9	10	11	12	13
Fire or explosion	Cargo tank hatches	Cargo tanks	Provide safe closure for major access opening to cargo tanks	Incomplete enclosure	• Wastage at sealing surface • Damage to sealing surface	Creates barrier-free vapor path to tank interior	si/f & mpd due to fire or explosion in tanks	• Explosive mixture in tank • Source of ignition in vicinity of faulty hatch	IV	Moderate	3	Critical
	Main deck cargo piping and valves	Cargo transfer system	Convey cargo between manifold connections and tank piping during both loading & unloading	Leakage	Wastage--especially at joinings	Release of cargo to open deck	i & pd due to small fire at leak area	• Source of ignition near drips area	III	Strong	2	Mandatory
				Rupture	Weak spot in piping due to local wastage or damage	Large release of cargo to open deck	si/f & mpd due to major fire on main deck	• Source of ignition near spill area	IV	Strong	2	Mandatory
	Cargo tank piping and valves	Cargo transfer system	Convey cargo to and from cargo tanks	Piping leaks	Wastage	Creates leakage path into other cargo tanks than the one served	si/f & mpd due to cargo tank fires	• Leak is into empty tank • Explosive mixture forms in leaking tank	IV	Moderate	3	Critical
				Piping rupture	Metal fatigue							
				Valve leakage	Wear	Creates open flow path into tank from piping system	si/f & mpd due to fire or explosion on main deck after overflow during filling	• Tank overfills • Source of ignition present	IV	Moderate	3	Critical
	Main cargo pumps (in pump room)	Cargo transfer system	Pressurize transfer system	Cargo leak to bilges	• Shaft seal failure	Cargo accumulation in pump room--possibility of an explosive mixture	si/f & mpd due to fire or explosion in pump room	• Formation of an explosive mixture • Ignition source	IV	Weak	3	Routine
	Main cargo deepwell pumps	Cargo transfer system	Pressurize individual cargo tank transfer system	Cargo leak to topside environment	• Shaft seal failure	Cargo release--possibility of explosive mixture developing in topside area	si/f & mpd due to fire on main deck area	• Formation of an explosive mixture • Ignition source	IV	Weak	3	Routine
	Pump room piping & valves	Pump room	Provide manifolding function for pump room pumps	Leaks	• Wastage • Fatigue failure	Leakage to pump room bilges--possibility of an explosive mixture	si/f & mpd due to fire or explosion in the pump room	• Formation of an explosive mixture • Ignition source	IV	Moderate	3	Routine

FIGURE 4-14. (Continued)

HAZARD MODE	ITEM IDENTIFICATION		FUNCTION	FAILURE/ERROR MECHANISM		EFFECT		SIMULTANEOUS EVENTS OR CONDITIONS REQUIRED	INSPECTION CRITICALITY EVALUATION			INSPECTION CRITICALITY LEVEL ASSIGNMENT
	ITEM	SUBSYSTEM		F/E	CAUSE	IMMEDIATE	ULTIMATE		HAZARD SEVERITY CATEGORY	INSPECTION IMPACT ON F/E PROB.	MULTIPLE EVENT RANKING	
1	2	3	4	5	6	7	8	9	10	11	12	13
Fire or explosion	Pump room lighting	Pump room	Provide safe illumination of space	Overheat so as to provide a source of ignition	• Damaged or off-spec. lamp cover • Incorrectly installed lamp cover	Ignition source in pump room	si/f & mpd due to fire or explosion in pump room	• Formation of an explosive mixture	IV	Moderate	2	Critical
	Pump room exhaust vent blower	Pump room	Pressurize exhaust vent system	Shutdown	• Electrical failure • Mechanical failure	Loss of air change in pump room--possible buildup of explosive mixture	si/f & mpd due to fire or explosion in pump room	• Cargo accumulation in bilges • Source of ignition	IV	Strong	3	Critical
				Sparking-ignition source	• Electrical malfunction	Creates ignition source in exhaust trunk--possibility of flashback into pump room	si/f & mpd due to fire or explosion in pump room	• Formation of explosive mixture in pump room	IV	Moderate	2	Critical
	Pump room exhaust vent trunk	Pump room	Contain and direct exhaust vent airflow	Holes in ducting causing short circuiting of air flow	Wastage	Loss of air change in lower part of pump room--possible buildup of explosive mixture	si/f & mpd due to fire or explosion in pump room	• Formation of explosive mixture in pump room • Source of ignition	IV	Strong	3	Critical

FIGURE 4-14. (Continued)

main and pumps are not part of the cargo system so the need for inspecting them as an integral part of controlling fire/explosion hazards in the cargo system did not emerge in the findings from the HMEA. In this respect, the logic diagram technique is superior to the HMEA when a limited scope safety analysis is to be performed.

The specific results of the HMEA, in the form of a safety critical profile, are presented in Figure 4-15. It will be noted that the results are similar to those obtained with the logic diagram technique except for the coverage limitations. In spite of the probability that there was subconscious biasing of the results with those of the logic diagram approach, the study team is satisfied that either of these analysis techniques, used in a qualitative manner, will produce similar results.

4.5 CRITIQUE OF ANALYSIS TECHNIQUES

The conduct of this study was successful with respect to the issues posed at the outset concerning analysis techniques. The study team arrived at a set of conclusions regarding these issues. The underlying questions being addressed were

- Does the system safety analysis approach work? Is it analytically satisfying, convenient to use, and are the results convincing?
- Does one or another of the analysis techniques available seem to be superior for use in the context of commercial vessels?
- What is the impact of the prospective use of system safety analysis techniques on the design of VIIS?
- Taken as a whole, do the results of this study shed any light on whether or not system safety techniques are better than conventional approaches to safety analysis and risk management for commercial vessels?

4.5.1 Tractability of the System Safety Approach

In the context of commercial vessel technology, the system safety approach proved to be entirely tractable for the study team involved. The

DATE/ _____ VESSEL SAFETY CRITICAL PROFILE PAGE 1 OF 1

ITEM	INSPECTION	HAZARD
	A. MANDATORY INSPECTION ITEMS	
CARGO TANK VENT PIPING	FUNCTIONAL & MATERIAL COND	OPENINGS INTO TANKS
MAIN CARGO DECK	WASTAGE--PLATING/WELDED FEAT	OPENINGS INTO TANKS
CARGO TANK BULKHEADS	MAT COND RE WASTAGE/CRACKS	NEXT STAGE LEAKAGE
MAIN DECK CARGO PIPING	MAT COND RE WASTAGE/CRACKS	LEAKS TO TOPSIDE
	B. CRITICAL INSPECTION ITEMS	
FLAME SCREENS	WASTAGE OR DAMAGE	VAPOR PATH TO TANKS
CARGO TANK HATCHES	MAT COND--DAMAGE	NONCLOSURE OF TANK
CARGO TANK ULLAGE FTGS	WASTAGE OR DAMAGE	NONCLOSURE OF TANK
CARGO TANK PIPING/VALVES	MAT COND--LEAKAGE	LEAK INTO CARGO TANK
PUMP RM LIGHTING	INSTALLATION--BREAKAGE--HOT	HOT SPOT IGNITION SOURCE
PUMP RM EXH VENT BLOWER	MECH COND--ELECT INSULATION	SHOTDOWN--SPARK DISCH
PUMP RM EXH VENT TRUNK	MAT COND--WASTAGE	AIR LEAK

COMMAND/_____ RESPONSE/_____

FIGURE 4-15. SAFETY CRITICAL PROFILE

process of breaking down the vessel systems into coherent, analyzable elements proceeded without difficulty. There were no contradictory or anomalistic interface problems. Although many interdependencies exist with respect to hazardous conditions and the means for controlling them, these were not severe and did not pose special analytical difficulty. Each of the three techniques used (PHA, logic diagram analysis, and HMEA) was applied without undue trouble to the STUDY VESSEL. Input information needed for these qualitative analyses was readily extracted from the vessel's plans, records, and other documentation; and from the insights gained in the course of the on board inspection and study. The underlying logic of each of the techniques was not defeated in application by excessive system complexity.

All the techniques were analytically satisfying; that is, the analysis process, in every case, suggested items to be covered that would not otherwise have been covered and exposed relationships that might not have been perceived by subjectively applied expertise. In other words, the use of systematic analysis techniques is believed to have obtained results that would not otherwise have been obtainable. The techniques were easy to use and flexible in application. At no time did the analysts have to "fight the method" instead of concentrating on the problem of identifying and assessing hazards.

Finally, in the judgement of the study team, the results are convincing. They generally satisfy one's intuitive ideas of what items on the STUDY VESSEL are most important to be inspected. In the few cases where intuition was surprised by the analytical results, the analyses provided satisfactory rationales for the seeming anomalies. For example, one would have expected the fire main and fire pumps to have been assigned top (mandatory) priority as inspection items in a study concerned with fire hazards. In fact, these items in the second (critical) ranking group; they are multiple-path failures with comparatively less likelihood of causing major damage or injuries in connection with a fire.

4.5.2 Most Useful Techniques

In considering the question of which of the analysis techniques is the most useful, one should note that, as explained in Section 4.2, the PHA is essential to any systematic safety analysis. It's relative usefulness is not, therefore at issue in this study.

As between the logic diagram and HMEA techniques, the following observations were made by the study team.

4.5.2.1 Data Responsiveness. Both techniques were useful and usable in arriving at convincing results in spite of the absence of quantitative data on failures.

4.5.2.2 Interplay of Techniques. Both techniques are actually in use at all times during the conduct of the safety analysis. If the analyst's basic strategy is to use the deductive technique, he will find himself using inductive tactics in carrying out that technique and vice versa. Thus, the techniques are not mutually exclusive; in fact, they are highly complimentary from the standpoint of the mental processes in play as the analysis goes forward. The real issue, frequently, has to do with which form of notation seems to be the most useful way to document and describe the results of the analysis.

4.5.2.3 Advantages and Disadvantages of the Logic Diagram Technique. In the opinion of the project team, the logic diagram technique has several great advantages: (1) it portrays the hazards more accurately and completely, (2) it explicitly depicts multi-path accidents so the criticality of the failures/errors involved can be accurately appraised, (3) it provides greater intellectual stimulus for creative safety analysis, and (4) it lends itself to quantitative solutions when and if data become available. The overriding advantage, however, is that the mathematical rigor inherent in the logic diagram technique imposes a practical discipline on the conduct of a qualitative approach such that one naturally develops the confidence in the results obtained. The disadvantage of the logic diagram technique is that the same

rigor alluded to above makes the job of designing the tree very demanding. It takes a long time to do, requires a great ability to conceptualize in both mathematical and engineering contexts, and forces the analyst to spend some amount of time on aspects of the safety problem in which he might have no immediate interest because the technique demands comprehensive treatment.

4.5.2.4 Advantages and Disadvantages of the HMEA. In these characteristics, the HMEA is in many respects the opposite of the logic diagram. Its advantages are: (1) it is a highly flexible, even subjective, tool so the analyst is free to tailor its format (table headings) to fit his particular needs, (2) he may arbitrarily restrict his study to only the particular set of failures/errors with which he is concerned thus avoiding irrelevancy, (3) there is greater scope for subjective judgement in making necessary assessments, and (4) it is a good communications tool because it is largely self explanatory--one need not be acquainted with boolean algebra to grasp its meaning. Its disadvantage is that, in this case at least, it offerred far less stimulus to describe accident possibilities completely, did not account for as many failures/errors, and does not explicitly depict the number of paths involved in generating an accident. Although a column entry was provided to account for this last factor, it was still judged that the HMEA's power to describe the interractions involved in developing an accident fell far short of that of the logic diagram.

4.5.2.5 Conclusions Regarding Analysis Techniques. On balance, the study team considers the logic diagram the more powerful tool and recommends its use where resources and time permit. However, the HMEA should never arbitrarily be eliminated from consideration and the natural interplay of the two techniques should be capitalized on when possible.

4.5.3 Impact of System Safety Analysis on the Design of VIIS

The impact on the design of VIIS was described fully in Section 3.6. Appendix C describes the implementation plan for incorporating in VIIS the capabilities that respond to the needs of system safety analysis of ships.

4.5.4 Superiority of System Safety Techniques

One of the results of this study is that the team is convinced of the superiority of the system safety approach in comparison with conventional methods of dealing with risk in commercial vessels. This is true in spite of the fact that the study did not turn up startling or dramatic new hazards. Review of the hazards listings in Table 4-3 in the light of the general literature and body of knowledge on the hazards of fire in vessels shows that almost no unknown or unsuspected hazards pertaining to ships of the STUDY VESSEL's type were found nor were any new, improved methods of hazard control revealed. It has been suggested that the hazards listings could have been developed without having to use system safety analysis techniques simply by querrying experienced individuals familiar with the STUDY VESSEL.

A basic question arises from this; namely, can the results of this study be interpreted to affirm or deny the premise mentioned in the "Introduction" to this report that system safety analysis techniques comprise a potentially superior way of managing risk with respect to commercial vessels and, therefore, should soon be incorporated in the Coast Guard's CVS program? Addressing this question is not precisely within the scope of this study. However, the matter is important and the study had results which, in the opinion of the study team, are pertinent to the question.

In measuring the effectiveness of safety analysis approaches, two criteria apply: (1) the efficacy of the approach in identifying hazards that are present in the system and (2) the ability of the methodology to provide a good basis for allocating resources for controlling the hazards.

4.5.4.1 Hazard Identification. In applying this criterion, the basic issue is the ability to identify hazards that have not yet been revealed by accidents and demonstrate their presence convincingly enough that scarce resources will be committed to controlling them. Those who advocate the use of system safety techniques claim that these techniques are effective in doing this whereas the "traditional" approach to safety engineering is purely reactive, spending resources to control only those hazards revealed by accident experience.

An example study of the kind conducted here cannot obtain a clear-cut answer on this matter. If, on the one hand, a vessel about which a body of experience already exists is studied, as in this case, it can be anticipated that the hazard field has already been well covered by that experience and there are, in fact, no new hazards of major importance remaining to be discovered. In that case, system safety techniques are useful mainly to organize the experience so as to maximize its usefulness in hazard control and to confirm that unknown/unsuspected hazards are not present. On the other hand, if the example study is directed to a vessel featuring novel technology about which there is no body of experience, the validity of the hazard listings produced by the study cannot be "proved". One can only speculate on the basis of how convincing the supporting analysis brought forward for the hazards are.

As between these two approaches, it was believed that, in this case, more useful insights about the application of system safety techniques could be drawn from taking the first. Although unsuspected hazards were not discovered, it is by no means unimportant that the study team identified and dealt with over 70 specific hazard conditions which span the field of experience pertaining to the scope of this study. The team members are analysts with marine experience but this experience is not in the field of designing, building, or operating vessels of the type studied here. The hazard listings cited in this report were developed through the use of system safety analytical procedures. Although these procedures included, as a matter of routine, accident experience*, the major source for the identification of

* The STUDY VESSEL itself has not experienced any fires or explosions in its 10-year service life.

specific hazards was the analytical process itself--vessel familiarization followed by the exploratory construction of accident logic diagrams and the HMEA tables. The resulting hazard listings are believed to recite accurately the experience compiled with respect to the topics covered in the study. This is interpreted by the study team as being strong confirmation of the capability of system safety analyses techniques to stimulate exhaustive hazard identification.

4.5.4.2 Basis for Resource Allocation. The SCP developed in this study is a resource allocation plan, the resource consisting of Coast Guard inspector manpower and material plus inspected vessel downtime costs. The SCP indicates how this particular resource can be most effectively deployed for the control of the observed hazards. The same system safety analysis techniques could be used to generate allocation plans for hazard control through vessel design, hazard control through law enforcement, and so on.

There is no counterpart to this capability in traditional approaches to safety assurance. Allocation of resources to safety were, and still are for the most part, made in a haphazard way mainly responding to accidents or incidents. Indeed, the main stimulus for the development of the system safety approach was the need for allocating resources to safety on a more rational and anticipatory basis in connection with new and novel systems in the space and defense domains.

The SCP developed herein demonstrates the capability of system safety techniques to support this decision-making function in the domain of commercial vessels. There is no other approach available. As the Coast Guard continues its endeavor to order its whole framework of safety activity into the most effective form, it will inevitably take up progressively the practice of system safety techniques.

APPENDIX A

TABLE OF CONTENTS

	Page
STUDY VESSEL DESCRIPTION	A-1
History	A-1
Service	A-1
Operating Phases	A-2
Cargoes Carried	A-3
Particulars	A-4
Hull	A-4
Boilers and Pressure Vessels	A-4
Propulsion	A-5
Mooring/Anchoring	
Navigation/Communications	A-5
Transmitting Equipment	A-6
Electrical	A-6
Life Protection	A-6
Fire Control	A-8
Cargo System	A-9

LIST OF FIGURES

Figure A-1. Cargo Tanks and Piping Schematic	A-10
Figure A-2. Cargo Pumping System Schematic	A-11

APPENDIX A

STUDY VESSEL DESCRIPTION

The STUDY VESSEL is a modern, high-speed special products carrier. Proper understanding of this safety analysis requires an adequate description of the ship in terms of general matters concerning the nature of her service and history, and the particulars of her several systems.

History

The STUDY VESSEL was built at the Sparrows Point shipyard of Bethlehem Steel and was placed in service by her present owners in 1966. Although the hull design was basically a standard Bethlehem item, the tank segregation details, cargo piping and pumping arrangements, and a variety of other features were worked out as a joint enterprise by the vessel owner, the prospective long-term charterer, and Bethlehem. The result is a vessel design unusually closely tailored to the requirements of a cargo movement operation that is precisely defined as to material hauled, schedule, and route.

The vessel has operated solely in the mode for which she was designed since going into service.

Service

The STUDY VESSEL hauls a large variety of high-value, liquid bulk products--refined petroleum products and chemicals--on a fixed route between a port on the Gulf Coast and a terminal at a petrochemicals processing complex in the Northeast. The full round trip, including loading and unloading, takes approximately 12 days; the northbound is the loaded run while the southbound is in ballast with tank cleaning and preparation operations being performed.

In performing this highly repetitous operation, the STUDY VESSEL is really functioning as an extremely critical materials handling step in a

continuous-flow chemical processing plant whose upstream part is in the Southwest while the downstream part is in the Northeast. Schedule variation allowances and delivered product purity requirements are tight in order to preclude expensive interruptions to the continuity of the overall process. Thus, the profit level for the vessel's owner depends on keeping the ship operation at a high level of reliability.

One of the complicating factors in the operation is that, although the spectrum of types of cargoes carried is well defined (the vessel was designed with this spectrum firmly established), there is still considerable variety from trip to trip in the specific loads carried. This means that on every southbound trip a substantial amount of tank cleaning and preparation is required to accommodate changes in the material to be loaded in certain of the tanks for the next trip. Although cargo schedules as to kinds and amounts for each trip are mapped out well in advance, there are characteristically a few last-minute changes communicated to the vessel during the southbound voyage; these have to be accommodated by changes in the cleaning and preparation operation while still at sea before arrival at the loading terminal.

Operating Phases

For safety analysis purposes, it was necessary to subdivide the total operation into phases, each of which represents a unique situation with respect to the several hazards. After considerable experimental iteration, the following operational phases were distinguished:

(1) Loading cargo at terminal in vicinity of population centers

(2) Unloading cargo at terminal in vicinity of population centers

(3) Underway, loaded, on soundings (entering or leaving harbor) near population centers

(4) Underway, unloaded and in ballast, on soundings (entering or leaving harbor) near population centers

(5) Underway, loaded, at sea, routine weather conditions

(6) Underway, loaded, at sea, heavy weather conditions

(7) Underway, in ballast, at sea, routine weather conditions

(8) Underway, in ballast, at sea, heavy weather conditions

(9) Underway, unloaded, at sea, cargo tank cleaning/ preparation operations being conducted.

Cargoes Carried

The STUDY VESSEL is certified by the Coast Guard to carry the following cargoes:

(a) Polar Solvents

Dimethyl Keytone (DMK)
Methyl Isobutyl Keytone
Methyl Isobutyl Carbinol
Methyl Ethyl Keytone (MEK)
Isobutyl Alcohol
Ethyl Alcohol
Ethylene Glycol
Normal Butyl Alcohol
Secondary Butyl Alcohol

(b) Other Cargoes

Petroleum and Lube Oils
Glycerine
Mineral Spirits
Naphtha
Benzene
Tolusol (Toluene)
Xylene
Styrene
Neodol
Epichlorohydrin (ECH).

In this listing, the category "petroleum and lube oils" covers all grades of gasoline, aircraft fuels, and many grades of lubes.

Particulars

Details of the STUDY VESSEL are presented here in terms of the vessel system breakdown defined in Appendix A.

Hull

The basic hull dimensions of the STUDY VESSEL are as follows:

Length overall - 660'-2"
Breadth (MLD) 90'-0"
International summer draft - 36'-7-3/4".

The hull arrangement is conventional. There is one ballast tank forward. The middle body contains the cargo tanks as will be described later in the "Cargo Systems Description". Main machinery spaces, fuel and water tanks, living quarters, and navigation bridge are aft.

The hull scantlings are ABS ship steel with heavy strakes of normalized plate in the way of the sheer strake and the main deck stringer plate in the middle body of the vessel.

The STUDY VESSEL is equipped with a Loderater analogue computer located in the Master's cabin. This equipment provided the Master with a means to predict static loads with various cargoes and distributions of such cargoes. The computer provides the following displacement/trim information:

Draft

Metacentric height

Static shear stress and bending moments at 10 locations along the ship's length.

Boilers and Pressure Vessels

Two Foster Wheeler, automatic combustion controlled boilers provide steam for the main propulsion and electrical service plants. Main propulsion steam is at 600 psi gage 900 degree superheat. Other pressure vessels are associated with the air conditioning system for the living quarters, the service compressed air system, and the fresh-water distilling plant.

Propulsion

The main propulsion system is steam turbine geared driving a single shaft with a three-bladed bronze propeller, 21'-6" diameter, 21'-8" pitch. The plant is rated at 15,000 shaft horsepower. The steam turbines reduction gear are General Electric units.

Mooring/Anchoring

The vessel is equipped with two stockless anchors (17,955 lb) plus one spare anchor. The anchors are linked to 330 fathoms of 2-13/16" stud link anchor chain. One electrohydraulic anchor winch with two horizontal wildcats handles the anchor chain.

Also provided on board is 900 feet of 2-1/8, 6 x 24 wire cable referred to aboard the vessel as an "insurance towline".

Other mooring equipment included six electrohydraulic, constant-tension mooring winches and one vertical electrohydraulic winch at the stern.

Navigation/Communications

The STUDY VESSEL was equipped with the usual equipment for terrestrial and celestial navigation. Equipment available included

- Sextants
- Azimuth circles
- Gyro and magnetic compasses
- An autopilot
- Radio direction finder (as noted below)
- Fathometer
- Loran A-C receiver
- Two radar systems (as noted below)
- Chronometers.

The following inventory of communications equipment was on board located in the radio room, bridge area, or elsewhere, as noted:

Transmitting Equipment

Type	Manufacturer	Type	Output Power, Watts
Telephone			
2M c/s	ITT/MM	216B	150
HF	ITT/MM	216B	150
VHF No. 1	Raytheon	Ray-42-VHF	25 O/P
VHF No. 2	INTECH	V 108	25 O/P
Radar #1	Raytheon	1650	n.a.
Radar #2	Kelvin Hughes	17/6us	n.a.
Telegraph			
Main	ITT/MM	2012A	1050
Emergency	ITT/MM	2010A	90
HF	ITT/MM	2018A (2F)	900
Survival craft	ITT/MM	401A	15

Receiving Equipment

Main receiver	ITT/MM	3010B
Emergency receiver	ITT/MM	3001A
Auto alarm	ITT/MM	5002B
DF	ITT/MM	4004A

Electrical

The electrical system is powered by two ships service turbo generator sets and one emergency diesel generator. The turbo generators, originally used on a Navy battleship, are GE units, Type ATB-2, rated at 450 v, 250 kva, 1000 kw @ 3600 rpm. The emergency generator, driven by a Cummins NHS-6-IP engine, is an EM Type BRKT rated at 150 kw, 450 v.

The electrical distribution system is of conventional arrangement. The main control board located forward, starboard side in the engine room, is by Federal Pacific. Main feeders, distribution panels, and controllers for all cargo pump motors are grouped in the engine room upper-level starboard side.

Life Protection

Life protection equipment for vessel emergency situations consists of

2 - lifeboats, 37-man capacity, fully equipped as prescribed in Coast Guard regulations

- inflatable rafts, automatic releasing, 36-man capacity, fully equipped as prescribed in Coast Guard regulations.
- life jackets.

Life Support. Life support (breathing equipment, including protective clothing, is provided for fighting fires and cleaning up spills of poisonous or combustible cargoes. Protective clothing and life support are also required when handling specially hazardous cargoes. The equipment is utilized in entering cargo tanks to determine the safety of the environment and to rescue personnel who may have been overcome in supposedly gas-free or safe atmospheres in tanks, pump room, or other enclosed spaces. Resuscitators are also carried for emergency treatment of casualties.

Life support equipment provided includes the following items:

Two Gas Masks, Type N. MSA Window Cator Model SW, cannister type for use with acids, ammonia, carbon monoxide, organic vapors, and particulates. This mask must not be used in oxygen-deficient atmosphere or to fight fires.

Two reflective fire-fighting personal protective suits including boots and gloves.

One oxygen Breathing Apparatus OBA plus spare oxygen cannisters.*

Two Air Masks MSA equipped with pressure regulators and air flasks.*

Two suits of chemical protective clothing plus goggles and gloves.

One resuscitator with spare oxygen bottles.

One MSA Foille Burn Kit.

Emergency Alarms and Machinery Shut-Down Equipment. There are 24 alarm bells distributed throughout the ship. These can be sounded at three stations - the navigation bridge, the passageway outside the Chief Engineer's office, and the engine room log desk or control station.

* Both of these equipments are provided with a harness and stainless steel cable life lines.

Ship's ventilation shut-down stations are located on the navigation bridge and log desk in the engine room.

Emergency stops for forced draft blowers, fuel oil service pumps, fuel oil transfer pumps, machinery space, and pump room ventilation systems are located on the starboard side passage way in the crew's quarters.

Fire Control

The fire control system on the STUDY VESSEL consists of three main means of fire fighting: (1) a conventional pressurized sea water system consisting of pumps, fire main, and associated hoses and application equipment; (2) a foam system consisting of a foam-generating plant, deck monitors, and application systems in pump room and engine room; and (3) a distributed fixed/portable system using CO_2.

Foam System. This system provides fire-fighting capability for the engine and pump rooms and the cargo area. Protection for petroleum fires and polar solvent fires are provided by 3 percent and 100 percent concentrate Aerofoam distribution systems. For petroleum fires, a 3 percent concentrate is used. For polar solvents, 100 percent concentrate is used in conjunction with the 3 percent concentrate.

Foam is controlled at the storage tank (1,365 gallons) and proportioning pump station located on the main deck in the forward part of the deck house on the center line. Sound-powered phones are used to control the system between this station, the bridge, the engine room, and the foam stations.

Foam is distributed by a 6-inch main to the main deck catwalk where there are four monitor stations. In addition, at each monitor there are 2-1/2-inch hydrants supplied with two portable foam nozzles. A 3-inch main can provide foam to the cargo pump room where 6 fixed nozzles distribute foam at the lower machinery level. A 6-inch main provides foam to 12 fixed nozzles at various locations in the engine room lower level.

AD-A046 288 BATTELLE COLUMBUS LABS OHIO F/G 13/10
SYSTEM SAFETY ANALYSIS OF A COMMERCIAL VESSEL.(U)
NOV 77 E S CHEANEY, A J COYLE DOT-CG-42087-A
UNCLASSIFIED BATT-G-2955-0001 USCG-D-39-77 NL

2 OF 2
AD
A046 288



END
DATE
FILMED
12-77
DDC

CO_2 Extinguishing Capabilities. One Walter Kiddie 100-lb cylinder with 50' of 1/2" hose with a nozzle and reel are located in the engine room. Twenty-six 15-lb portable CO_2 extinguishers are located throughout the ship. The paint locker and the cargo office are protected by fixed CO_2 systems.

Firemain Systems. The firemain is a single 8" pipeline running fore and aft. There are no isolation valves in the firemain. The system is served by two electrically-driven fire pumps of 600 gpm capacity. An 800 gpm steam-turbine-driven pump can also pressurize the firemain. However, this last pump is used mainly for tank cleaning. The firemain serves 22 fire stations equipped with all-purpose nozzles, low-velocity applicators, and a total of 1575' of 2-1/2" and 1-1/2" hose.

Equipment Installed But Not Required by Regulations. Ten ANSUL portable dry chemical fire extinguishers (38-lb capacity) are provided and located close to the cargo transfer manifolds on the main deck when cargo is being pumped between ship and shore. Two ANSUL dry chemical extinguishers of 150-lb capacity are installed in 3 CP and 4 C pump houses on the main deck.

Cargo System

Figures 4-2 and 4-3 are deidentified copies of the standard descriptive form used aboard the STUDY VESSEL for planning cargo operations. The two figures provide a complete physical and operational description of the cargo system which consists of tanks, pumps, and associated piping, fittings and auxiliary equipment. Examination of the vessel showed no discrepancies in these drawings.

STOWAGE PLAN-PUMPING FACILITIES

This form is to be prepared in triplicate for each cargo loaded - one copy to be sent to the office - one copy to be airmailed to the discharging terminal - one copy to be retained on board for the ship's files.

Voyage No._____ Loaded at_____ Date_____

Discharg_____ Date_____

6P	5P	4P	3P	2P	1P
15,780	17,268	11,893	11,877	10,663	13,287
6CA 6CP 1261 25,308	5CA 5CP 5CS 13451 6693	4C 24,686	3CP 3CA 3CS 6717 6715	2CA 2CP 2CS 6707 6709	1C 33,942
6S 15,830	5S 17,290	4S 11,890	3S 11,892	2S 10,664	1S 13,286

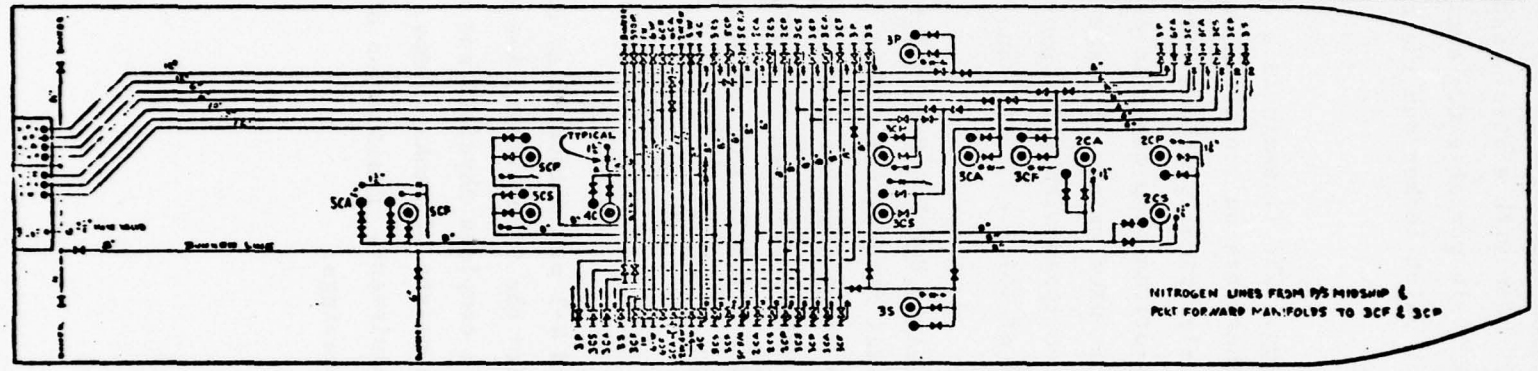
SEGREGATIONS & CAPACITIES IN BARRELS 100% FULL

Color	Product	Quantity (Bbls)

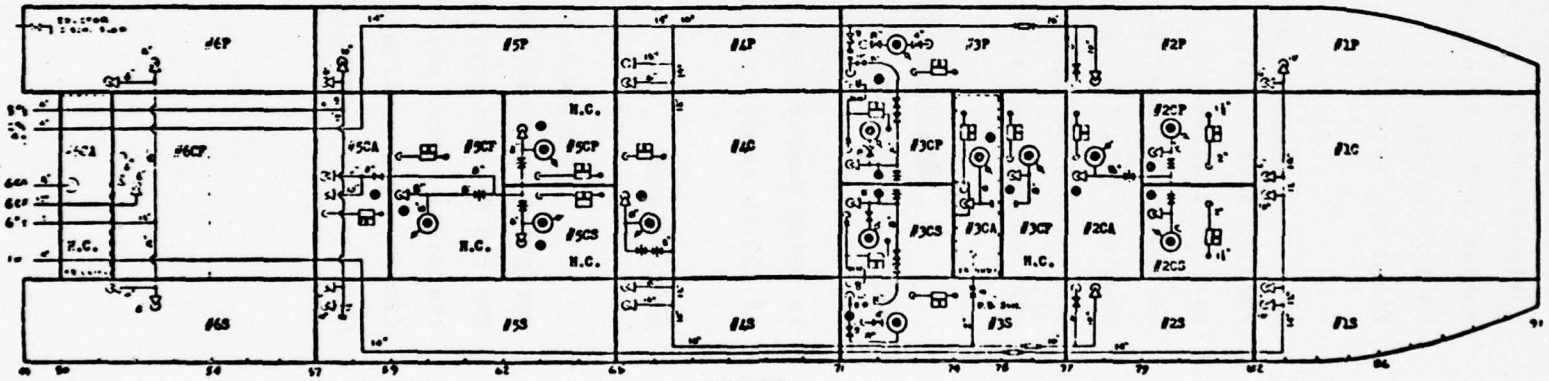
Color Squares to correspond to Fig. 1 and show Product and Quantity of cargo loaded

LENGTH OVERALL:- 660'-2" BREADTH (MLD):- 90'-0"
INTERNATIONAL SUMMER DRAFT:- 36' 7-3/4"
Center of Manifold to Bow 304'-2", to Stern 356'-0"

HEADER	SIZE	PRODUCT	PIPING COLOR	MATERIAL	TYPE
3CP	8"	Chemicals	1-Blue	Aluminum	D.W.
3CA	8"	Chemicals	2-Blue	Aluminum	D.W.
3CP	8"	Chemicals	3-Blue	Aluminum	D.W.
3CS	8"	Chemicals	4-Blue	Aluminum	D.W.
3P	8"	Chemicals	5-Blue	Aluminum	D.W.
3S	8"	Chemicals	6-Blue	Aluminum	D.W.
2CP	8"	Oil Solv.	1-Green	Aluminum	D.W.
2CS	8"	Oil Solv.	2-Green	Aluminum	D.W.
2CA	8"	Oil Solv.	3-Green	Aluminum	D.W.
5CP	8"	Lube Oil	1-Orange	Steel	D.W.
5CS	8"	Lube Oil	2-Orange	Steel	D.W.
5CP,5CA	8"	Lube Oils	3-Orange	Steel	D.W.
6CA	6"	Glycerine	1-Red	Aluminum	D.W.
1P,1C,1S	12"	Petroleum	1-Yellow	Steel	E
2P,2S,4P,4S	12"	Petroleum	2-Yellow	Steel	B
6CP	10"	Petroleum	3-Yellow	Steel	C
4C	8"	Petroleum	4-Yellow	Steel	D.W.
5P,5S	12"	Petroleum	5-Yellow	Steel	A
6P,6S	10"	Petroleum	6-Yellow	Steel	D
Stripping	6"	-	-	Steel	-
Number	8"	-	-	Steel	-



DECK LINES



TANK LINES

FIGURE A-1. CARGO TANKS AND PIPING SCHEMATIC

RECORD OF SEALING VALVES

Voy. No. _____ Date _____ Port _____

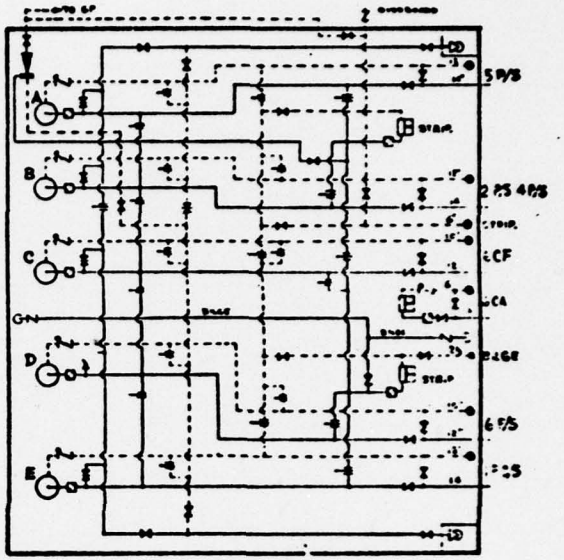
The Master, Mates and Pumpmen should become familiar with the entire cargo pipeline system, the pumproom facilities, and the blinds, blanks, valves, etc., in association therewith.

To prevent cargo from being accidentally discharged overboard, or contamination of one product by another, the diagrams in Figs. 2, 3 and 4 should be studied for the purpose of deciding which valves should be opened, closed, or closed and sealed, to safely and properly load or discharge each individual parcel. Mark X each valve closed, and O each valve sealed, and list in space provided below.

LIST BELOW ALL VALVES WHICH HAVE BEEN SEALED IN EITHER PUMPROOM OR DECK		
Location of valve	Name of valve	Seal No.

SYMBOLS	
	Centrifugal Pump
	Deep Well Pump
	Reciprocating Pump
	Eductor
	Gate Valve
	Double Disc Gate Valve
	Angle Valve
	Check Valve
	Drain Valve
	Riser Line Blind
	Strainer
	Riser/Drop Lines
	Expansion Joint
	Spool Cut/Line Blanked
	Spectacle Blind
	Line Blanked
	Pump Room Disch. Lines
N.C.	Heating Coils

PUMPROOM FACILITIES



CARGO PUMPS				
	TYPE OF PUMP	DRIVER	DISCHARGE RATE	H.P.
	Centrif.	440 V Motor	6857 bbls/hr	600
	Centrif.	Steam Turb.	6857 bbls/hr	600
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1500 bbls/hr	125
	Centrif.	440 V Motor	1500 bbls/hr	125
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1500 bbls/hr	125
	Centrif.	440 V Motor	1500 bbls/hr	125
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1286 bbls/hr	100
	Centrif.	440 V Motor	1500 bbls/hr	125
	Centrif.	Steam Turb.	4000 bbls/hr	385
	Centrif.	Steam Turb.	4000 bbls/hr	385
	Centrif.	Steam Turb.	1000 bbls/hr	Steam
	Centrif.	Steam Turb.	1000 bbls/hr	Steam

CARGO TANK COATINGS	
Tanks	Coating
1,2,4,5,6 Port & Stbd 1C, 4C 5CP,5CS,5CF,5CA,6CF	Sovopox (Epoxy)
3P, 3S 2CP,2CS,2CA 3CF,3CA,3CP,3CS	Dimetcote 9 (Zinc Silicate)
6CA	

STRIPPING SYSTEM (Diagram)			
		Pump Make, Size & Type	DRIVER DISCH.RATE
1CP,2CP,3CP,4CP,5CP, 1CS,2CS,3CS,4CS,5CS,6CS	12	Penn Brothers 4x2-5/8x5 Horiz. Recip.	Air 21.4 BPH
3P	1	Nevada Stainless Steel 3x3-3/4x4 Horiz. Recip.	Air 28.6 BPH
5CA	1	Union (Modified Stainless) 4x2-3/4x4 Horiz. Recip.	Air 21.4 BPH

FIGURE A-2. CARGO PUMPING SYSTEM SCHEMATIC

Preceding Page BLANK - NOT FILMED

APPENDIX B

STUDY VESSEL SYSTEMS

Preceding Page BLANK - NOT FILMED

APPENDIX B

STUDY VESSEL SYSTEMS

Below are tabulated the ship systems breakdown used in the safety analysis of the study vessel. This breakdown is the one used in the design of VIIS's data base. It is based on, and nearly identical to, a breakdown developed by MIS in 1974 as the frame work for the Casualty Reporting System.

VESSEL SYSTEMS

Level I	Level II	Level III	List No.
1. Hull	1. Watertight Envelope	1. Main Deck	1
		2. Penetrations	2
		3. Shell Plating	3
	2. Strength Members	1. Decks	4
		2. Frames	5
		3. Bulkheads	6
	3. Super-Structure	1. Decks	7
		2. Frames	8
		3. Bulkheads	9
	4. Water Removal/ Ballast M'gt.		55
2. Boilers & Pressure Vessels	1. Main Propulsion Boilers	1. Main Engine	10
	2. Auxilliary Boilers	2. Auto Regulating Systems	11
	3. Unfired Pressure Vessels	3. Steam Cycle	12
		4. Fuel Oil	13
		5. Lube Oil System	14
		6. Cooling System	15
		7. Air System	16
3. Propulsion	1. Power Generation System		
	2. Coupling System	1. Fluid	17
		2. Mechanical	18
		3. Electrical	19

Level I	Level II	Level III	List No.
Propulsion (Cont.)	3. Thrust System	1. Shaft	20
		2. Bearings	21
		3. Propeller	22
	4. Vessel Movement System	1. Steering Control	25
		2. Propulsion Control	26
4. Mooring/ Anchoring	1. Mooring		23
	2. Anchoring		24
5. Navigation/ Communications	1. Vessel Location system		24A
	2. Communication System	1. Interior	27
		2. Exterior	28
6. Electrical System	1. Power Generation	1. Generation System	29
	2. Emergency Power Generation Sys.	1. Emergency Generation System	31
		2. Emergency Drive Sys.	32
	3. Power Distribution	1. Safety System	33
		2. Power Feeder System	34
		3. Hotel Feeder System	35
		4. Emergency System	36
7. Life Protection System	1. Vessel Abandonment	1. Individual Protection System	37
		2. Group Participation Sys.	38
	2. On Board System	1. First Aid System	39
		2. Personnel Protection System	40
8. Fire Control	1. Fire Detection System	1. Electric System	41
		2. Pneumatic System	42
		3. Heat Detecting System	43
		4. Smoke Detecting System	44
		5. Manual Detection System	45
	2. Fire Fighting System	1. Fixed System & Semi-Portable	46
		2. Portable System	47
	3. Fire Containment System	1. Structures & Closures	48

Level I	Level II	Level III	List No.
9. Cargo System	1. Cargo Environment Control	1. Pressure Control	49
		2. Safety System	50
		3. Air Conditioning	51
	2. Containment Sys.	1. Primary Containment	52
		2. Secondary Containment	53
	3. Transfer System	1. Cargo Loading/Unloading	54
10. Habitability	1. Sanitary System	1. Salt Water	None
		2. Drainage	None
	2. Vessel Access System	1. Personnel Boarding	56
		2. Safety System	57
		3. Onboard	58
	3. Air Conditioning System	1. Heating	59
		2. Humidity	60
		3. Cooling	61
		4. Ventilation	62
	4. Food and Water System	1. Pest Control	None
		2. Food Preparation	None
		3. Food Consumption Facilities	None
		4. Food Storage	63
		5. Portable Water Supply	64
	5. Personnel Accommodation System	1. Sanitary & Recreation Facilities	None

COMPONENTS

List No.

1 Main Deck
- Damage
  - Forward Quarter
  - Mid-half Length
  - After Quarter
- Repair
  - Forward Quarter
  - Mid-half Length
  - After Quarter

2 Penetrations
- Deck Penetrations
  - Cargo Hatches
  - Ullage Openings
  - Scuttles
  - Manholes
- Shell Penetrations
  - Side Ports
  - Sea chests/sea suctions
  - Overboard Discharges
  - Transducers, fathometer, portholes & Other

3 Shell Plating
- Damage
  - Forward Quarter
  - Mid-half Length
  - After Quarter
- Repair
  - Foreward Quarter
  - Mid-half Length
  - After Quarter

4 Decks (below main deck)
- Level 1
- Level 2
- Level 3
- Level 4
- Tank Tops

5 Frames (below main deck)
- Longitudinal
- Transverse
- Vertical

List No.

6 Bulkheads (below main deck)
- Longitudinal
- Transverse
  - A. watertight subdivisions
  - B. other

7 Decks (above main deck)
- Level A
- Level B
- Level C
- Level D

8 Frames (above main deck)
- Longitudinal
- Transverse
- Vertical

9 Bulkheads (above main deck)
- Longitudinal
- Transverse
  - A. watertight subdivisions
  - B. other

10 Main Engine
- Casing/Block
- Blade/Piston
- Crankshaft, shaft rotor
- Bearings
- Intake/exhaust valves
- Sentinel valves

11 Auto-regulation System
- Combustion Control board
- Engine Room console
- Bell recorders
- Information Recorders
- Throttle control equipment
- Other

12 Steam Cycle
- Boiler
  - Tubes
  - Drums
  - Economizer/air heaters
  - Safety valves
  - Super heater
- Water heaters
  - DC heaters
  - Grease extractors
- Relief valves

List No.

12 (cont.)

Valves & controls
- Feed
- Stop
- Check
- Water level Indicators

Pumps
- Injectors
- Air ejectors

Gauges
- Thermometers
- Water Level Indicators
- Pressure Gauges

Condensers
- Main
- Auxiliary

Piping

13 Fuel Oil

- Pumps
- Valves
- Pipes
- Storage Tranks
- Vents & Strainers
- Injectors/Carburetors
- Heat Exchangers
- Gauges & Thermometers
- Alarms
- Remote Shutoff Valves
- Relief Valves

14 Lube Oil

- Pumps
- Valves & Controls
- Tanks
- Vents
- Strainers
- Heat Exchangers
- Piping
- Gauges & Thermometers
- Alarms

List No.

15 Cooling System
- Pumps
- Valves & Controls
- Heat Exchangers
- Tanks & Vents
- Piping
- Alarms
- Gauges & Thermometers

16 Air System
- Blowers
- Forced Draft Fan
- Turbo-charger
- Ducts
- Gauges
- Controllers
- Burner Air Register
- Stacks/Exhaust Piping
- Alarms

17 Coupling System
- Fluid System
- Hydraulic System
- Air System
- Casing
- Bearings
- Shafting
- Pressure Relief Valves

18 Mechanical System
- Casing
- Gears
  - Bull Gear
  - Sprindle
  - Pinion
  - Other Gears
- Bearings
- Shafting

19 Electrical System
- Casing
  - Air Cooled
  - Water Cooled
  - Refrigerant Cooled
- Motor Generator
  - Coils
  - Windings
  - Brushes
  - Commutator
  - Shafting
  - Bearings
  - Rotor

List No.

19 (Cont.)

- Stator
- Armature
- Over Current Protection

20 Thrust System
- Shafting
  - Line Shaft
  - Tail Shaft
  - Key
  - Keyway
  - Sleeves

21 Bearings
- Thrust Bearing
- Stern Tube Bearing
- Spring Bearing

22 Propeller
- Blades
  - Fixed Pitch
    - Built up
    - Solid
  - Variable Pitch
- Pitch Control
- Propeller Nut
- Nozzles

23 Mooring & Anchoring System
- Mooring
  - Lines
  - Winches
  - Constant Tension Winch
  - Capstans
  - Rigging
  - Cleats
  - Bits
  - Winch Controls

24 Anchoring
- Chain/cable
- Anchor
- Windlass
- Hawse Pipe/cover
- Chain Locker
- Windlass Control/brake

24A Vessel Location System
- RDF
- Loran A or C
- Omega
- Radar
- Sextant

List No.

15 Cooling System
- Pumps
- Valves & Controls
- Heat Exchangers
- Tanks & Vents
- Piping
- Alarms
- Gauges & Thermometers

16 Air System
- Blowers
- Forced Draft Fan
- Turbo-charger
- Ducts
- Gauges
- Controllers
- Burner Air Register
- Stacks/Exhaust Piping
- Alarms

17 Coupling System
- Fluid System
  - Hydraulic System
  - Air System
  - Casing
  - Bearings
  - Shafting
  - Pressure Relief Valves

18 Mechanical System
- Casing
- Gears
  - Bull Gear
  - Sprindle
  - Pinion
  - Other Gears
- Bearings
- Shafting

19 Electrical System
- Casing
  - Air Cooled
  - Water Cooled
  - Refrigerant Cooled
- Motor Generator
  - Coils
  - Windings
  - Brushes
  - Commutator
  - Shafting
  - Bearings
  - Rotor

List No.

19 (Cont.)

- Stator
- Armature
- Over Current Protection

20 Thrust System
- Shafting
  - Line Shaft
  - Tail Shaft
  - Key
  - Keyway
  - Sleeves

21 Bearings
- Thrust Bearing
- Stern Tube Bearing
- Spring Bearing

22 Propeller
- Blades
  - Fixed Pitch
    - Built up
    - Solid
  - Variable Pitch
- Pitch Control
- Propeller Nut
- Nozzles

23 Mooring & Anchoring System
- Mooring
  - Lines
  - Winches
  - Constant Tension Winch
  - Capstans
  - Rigging
  - Cleats
  - Bits
  - Winch Controls

24 Anchoring
- Chain/cable
- Anchor
- Windlass
- Hawse Pipe/cover
- Chain Locker
- Windlass Control/brake

24A Vessel Location System
- RDF
- Loran A or C
- Omega
- Radar
- Sextant

List No.

24 Cont:
- Compass (Magnetic)
- Charts

25 Movement System
- Steering Control
  - Gyro Repeaters
  - Gyro Compass
  - Magnetic Compass
  - Iron Mike/Automatic Steering
  - Rudder Angle Indicator
    - Electrical
    - Mechanical
    - Alarms
  - Electrical Switches/Controllers
  - Motors
  - Pumps
  - Cylinder/Ram
  - Ships Wheel
  - Trick Wheel
  - Aft Steering Station
  - Alarms
  - Valves
  - Bow Thruster

26 Propulsion Control
- Engine Order Telegraph
  - Mechanical
  - Electrical
  - Alarms
- Bell Pulls
- Voice Tubes
- Bridge Console
  - Throttle Control
  - Directional Control
  - Condition Recorder
  - Bell Recorders
  - Information Recorders

27 Communication Systems
- Interior System
  - Telephones
    - Electric
    - Sound Powered
  - Voice Tubes
  - General Alarms
  - Public Address
  - Public Address (Emergency)

28 Exterior System
- Navigation Lights
- Flashing Lights
- Flares
- Rockets
- Radio

List No.

28 (Cont.)

Radar
Sonar
Fathometer
Whistles/Fog Horn/Siren

29 Power Generation System
Generation System
Battery
Electric Generator AC/DC
Over Currrent Protection
Reverse Current Relay
Other_____

Drive System
Steam Turbine
Gas Turbine
Diesel Engine
Gasoline Engine

31 Emergency Power System
Generation
Battery
Generator AC/DC
Safety Devices

32 Drive
Diesel Engine
Gasoline Engine
Gas Turbine Engine
Safety Devices

33 Distribution System
Safety System
Over Current Protection
Fuses
Circuit Breakers
Mats & Guards

34 Power Feeder System
Main Distribution Panel
Motor Controllers
Battery Chargers
Miscellaneous Small Motors
Switches
Power Panels
Wiring

List No.

35 Hotel Feeder System
- Lighting
- Electrical Panels/Distribution Boards
- Wiring
- Switches

36 Emergency System
- Emergency Power Panel
- Emergency Lighting Circuit
- Wiring
- Switches
- Over Current Protection

37 Vessel Abandonment
- Individual Protection
  - Life Jackets
    - How many required
    - How many found onboard
    - How many rejected
  - Ring Bouys/Lighted Ring Bouys/Line
  - Work Vests

38 Group Participation
- Life Boats
  - Hull & Fittings
  - Tank & Fittings
  - Equipment & Storage
- Life Rafts
  - Structure
  - Releasing Gear
  - Equipment & Storage
- Lifefloats & Bouyant Apparatus
- Disengaging Apparatus
- LifeBoat Propulsion
  - Motor
  - Hand Propelled
  - Oars
  - Sail
- Davits/Falls/Lifeboat winches/Controls
- Standing & Running Rigging
- Ladders & Lifelines
- Portable Radios
- Workboat

List No.

39 Onboard System
- First Aid
  - Hospital
  - Medicinal Supplies
  - Stretcher
  - Operating Room Explosion Proof

40 Personnel Protection
- Fresh Air Breathing Apparatus
- Self-contained Breathing Apparatus
- All Purpose Masks
- Emergency Squad Equipment
- Protective Clothing
- Flame Safety Lamp
- Explosion Proof Flashlight

41-45 Fire Detection
- Resistors
- Detectors
- Zone Indicator Panels
- Alarms
- System Control Panel (controls)
- System Test Panel
- Piping
- Valves
- Vent Controls
- Punch Clock
- Key & Holders

46 Fire Fighting
- CO_2 Storage Bottles
- Operation Controls
- Vent Controls
- CO_2 Alarm
- CO_2 Discharge Delay Mechanism
- Actuation
- Valve (Stop)
- Discharge Nozzle
- Pipe
- Hose
- Reels
- Fire Pump
- Emergency Fire Pumps
- Valves
- Hydrants
- All Purpose Nozzle
- Supply Tanks
- Proportioning System
- Foam Monitors

47 Portable Systems
- Container

List No.

47 (Cont.

Hose
Nozzle

48 Fire Containment
Closures & Structures
Stuffing Boxes
Fire Dampers (vents)
Valves
Spool Pieces
Fire Doors
Fire Door Controls

49 Cargo Environment Control System
Pressure Control
Safety/Relief Valves
Pressure/Vacuum Valves
Open Vent
Flame Screen
Piping

50 Safety System
Inerting System
Leak Detection Equipment
Liquid Level Gauging
Closed
Open
Restricted
Piping

51 Air Conditioning System
Temperature Control
Piping
Valves
Control Equipment
Ducting
Dampers
Heating Equipment/Steam/Electric
Fans
Refrigeration Equipment/Compressor

Humidity Control
Dehumidifier
Ducting
Control Equipment
Fans
Dampers
Valve

List No.

52 Containment System
- Primary Containment System
  - Single Skinned Cargo Holds
  - Single Skinned Liquid Tanks
  - Ullage Opening/Closure Fittings
  - Hatch Coaming
  - Hatch Cover
  - Hatch Closing Controls
    - Electric
    - Mechanical
    - Hydraulic
  - Pipes/Wires

53 Secondary Containment System
- Securing/Hold Down Devices
- Closures/Openings
- Barge/Container Skin Covering

54 Transfer System
- Cargo Loading/Unloading
  - Piping
  - Pumps
  - Valves
  - Winches
  - Booms
  - Cranes
  - Rotary Cranes
  - Gantry Cranes
  - Rigging (standing & running)
  - Elevators
  - Conveyors
  - Controls

55 Water Removal/Ballast System
- Piping
- Pumps
- Valves
- Controls

56 Vessel Access System
- Personnel Boarding System
  - Gangways
  - Pilot Ladders
  - Accommodation Ladders
  - Swing Ropes
  - Other_____

List No.

57 Safety System
- Gangway Safety Nets
- Rubber Mats
- Non-skid Deck/Ladder Coverings
- Hand Rails
- Grab Rails
- Warning Signs

58 Onboard System
- Ladders
  - Vertical
  - Inclined
  - Portable
- Passages
- Doors
  - Watertight
  - Weather/Exterior
  - Reefer
  - Interior
  - Fire
- Manholes
- Scuttles
- Working Platform/Staging/Boatswain Chair
- Floor Plate/Grating and Supports

59 Air Conditioning System
- Heating
  - Auxiliary Boiler
  - Hot Water Heater
  - Pipes
  - Valves
  - Fuel System
  - Radiators
  - Fans
  - Safety Valves
  - Relief Valves
  - Safety Controls
  - Pumps
  - Burners

60 Humidity
- Humidifiers
- Dehumidifiers
- Ducting
- Fans
- Controls

61 Cooling
- Compressors
- Pipes

List No.

61 (Cont.)

- Valves
- Motors
- Fans
- Ducts
- Cooling Agent
- Control Valves (Expansion, Solenoids)
- Evaporator Coils
- Receivers
- Condensers
- Controls

62 Ventilation

- Ducts
- Dampers
- Fans
- Coils
- Remote Securing Devices
- Fire Closures
- Controls

63 Food and Water

Food Storage

- Reefer Door Safety Latches
- Reefer Boxes
- Compressors
- Receivers
- Condensers
- Evaporator Coils
- Pipes
- Control Valves
- Gauges
- Dry Storage Areas

64 Portable Water Supply

- Shore Connections

Evaporator (H.P. or L.P.)

- Air Ejectors
- Condensers
- Control Valves
- Pipes
- Valves
- Pumps
- Relief Valves
- Test Equipment
- Gauges

APPENDIX C

SYSTEM SAFETY ANALYSIS RESULTS IMPLEMENTATION PLAN

APPENDIX C

SYSTEM SAFETY ANALYSIS RESULTS IMPLEMENTATION PLAN

In section 3.6 of the main body of this report, the safety analysis task's potential impacts on VIIS were described. Three requirements resulting from these impacts were identified:

- Ensure that VIIS is designed to have the capability for entry, updating, and retrieval of an SCP for each vessel in the system for which an SCP record is deemed appropriate.
- Ensure that VIIS can accumulate failure data from the field and search it in a manner useful for safety analysis.
- If judged appropriate by the Coast Guard, expand the plan for VIIS' analytical capabilities to include programs capable of solving problems involving symbolic logic diagrams representing Boolean algebra equations.

The implementation of these requirements has already been provided for in the basic VIIS Implementation Plan.* The first one, having to do with the SCP, simply presents the need to provide another user product in the system. Implementation Task I.1 "Finalize Design Products" has as its specific objective the design and incorporation of any new products thought necessary for VIIS at the outset of the implementation term. This task is scheduled to run during the first four months of that term.

There is some reason to doubt that it will be necessary to build the SCP capability into VIIS that early in its life. The Coast Guard's employment of system safety techniques in its vessel safety program will require some years yet before it matures to the point that vessel SCP's are coming into the information system. The fact is that VIIS has been designed with the capability in its own software to generate new user products and screen formats at any time. Therefore, the most reasonable implementation plan for the first item is to re-examine the need for the new product during Task I.1 and proceed accordingly.

---

* Citation of current issue of the "Implementation Plan".

Implementing the second item is more urgent. However, it has in fact already been implemented in the system in the form of the "Vessel File Damages/Defects Log" and the plan to include a general-purpose analysis capability to analyze the system's data base directly to seek and develop correlations among the data elements, and to conduct all standard statistical analyses.

The third item would best be implemented by adding one of the standard programs that have been developed for solving fault trees. It is not expected that this will become an urgent matter in the near future since it does not serve an objective arising from inspection function information needs.

APPENDIX D

LOGIC DIAGRAM CONSTRUCTION AND SYMBOLOGY

Preceding Page BLANK - NOT FILMED

APPENDIX D

LOGIC DIAGRAM CONSTRUCTION AND SYMBOLOGY*

A logic diagram analysis of an accident begins with the identification and definition of the accident in terms precise enough to support analytical treatment. The accident is then established as the "top-level undesired event".

The logic diagram is constructed to show symbolically the cause-effect relationships between the top-level undesired event and the contributing causes of its occurrence. It is a deductive analytical means to identify all failure modes contributing to the potential occurrence of the event. The logic diagram differs from the other main safety analysis techniques, the PHA and the HMEA, in that it displays all necessary failure modes and specific conditions which cause the top event, while the others consider only single mode relationships to the top event.

Logic diagrams can be developed in either qualitative or quantitative form. Every analysis using them begins as a qualitative analysis: most of the value of doing this kind of analysis is realized in this form. Hazards which might otherwise be missed are systematically identified. The quantitative analysis aimed at numerical evaluation of "how big is the problem" can be expensive in relation to the value of the information obtained and is often impractical to perform. The answers obtained are never better than the numbers and assumptions used in the analysis. If a specific tolerance level or limit is specified for the system, then a quantitative solution is necessary and the probability of the top undesired event and its individual contributing events are calculated. The quantitative logic tree provides the foundation for applying safety engineering effort to control or eliminate those contributing failure paths having the highest probability of occurrence. Such paths are generally described as "critical" or "dominant" paths and they indicate the single failure or the combination of primary failure modes (independent failure modes) which are most likely to actuate the top event.

---

* The description presented here is based on the treatment of the topic in "Weapon System Safety Guidelines Handbook: System Safety Engineering Principles, Part III", NAVORD OD 44942, Section 7.11, Naval Ordnance Systems Command, May, 1973.

While numerical techniques are useful for relative comparisons, their use in determining absolute values is generally meaningless. The implication that valid and reliable numbers are available ignores the fact that unpredictable interactions and the human element are invariably somewhere in the system being analyzed.

The logic diagram has become known as a "fault tree" in system safety usage. It is really a symbolic event logic diagram or a complex logical statement because its construction is based on symbolic logic principles. The top undesired event is represented by a proposition, and all other substatements describing related events are connected through logical constants or connectives. All elements are governed by the basic laws and definitions of symbolic logic and set theory. Figure D-1 gives the symbology usually employed in constructing the diagram and the meaning of each.

Logic Diagram Guidelines

The steps for performing the logic diagram analysis are listed in the following tasks:

(1) Define the top undesired event boundary
(2) Collect input data
(3) Construct the diagram
(4) Evaluate the diagram
    (a) Qualitatively
    (b) Quantitatively
(5) Summarize and report results
    (a) Undesired top event within the risk limit
    (b) Corrective action
        1. Verify results of corrective action
        2. Update diagram structure
    (c) As a rule, any fault in which an AND gate does not occur above the fourth (4th) level indicates that unwarranted hazards may exist in the system.

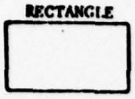
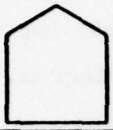
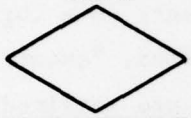
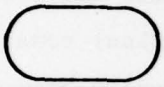
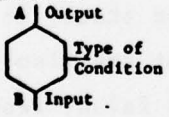
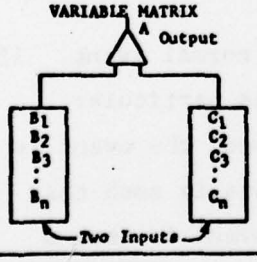
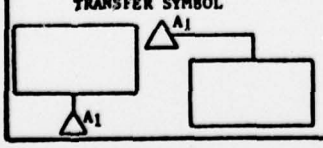
RECTANGLE 	This symbol represents the top undesired event or any intermediate event. Expressed in form of a proposition, statement set, or outcome of an observation.
CIRCLE 	A basic event requiring no further development for the purpose of analyzing the particular logic diagram. Defined as an "independent output" event or as a "primary" event.
HOUSE 	An event that must occur, or is expected to occur, as a normal operating condition of the system. It is not a failure or fault event.
DIAMOND 	An event arbitrarily treated as basic in a logic diagram so that it is not developed further.
OVAL 	An event that is a conditional input to a condition gate (see below). Defines a particular state of the system in which an input event may occur. It may be a normal condition or a failure.
AND  Two or More Inputs	An AND gate describes the logic operation whereby the coexistence of all input events is required to produce the output event.
Inclusive OR  Two or More Inputs	An OR gate describes the logic operation whereby the output event will exist if one and/or more of the input events exists.
CONDITION 	A "general inhibit" gate (or "condition" gate) describes a causal relationship between one event and another. The input event directly produces the output event if the indicated condition is satisfied. May be treated as an AND gate in logical analysis.
VARIABLE MATRIX 	A "matrix" gate describes a situation where an output event is produced for certain combinations of events at the inputs. Input combinations are indicated by a (1) in the diagonal squares of the matrix and (0) for all other squares. Only combinations having the value (1) are considered in the event combinations.
TRANSFER SYMBOL 	A transfer symbol is used to indicate continuity between two parts of a logic diagram. An alphanumeric symbol (A_1) indicates the part of the diagram to which, or from which, the transfer is made.

FIGURE D-1. LOGIC DIAGRAM ELEMENTS AND THEIR MEANINGS

Logic Diagram Symbology

As mentioned previously, the logic diagram is a symbolic event diagram or a composite statement made by connecting substatements, using applicable logical constants to imply cause-effect relationships. It relies heavily on symbology to assure consistency throughout the diagram, to aid in identification of and reference to substatements, propositions, and logical constants, and to simplify the flow of thought projected by the diagram.

The terms,"composite statement", "substatement", and "proposition", refer to the statements used in describing the top or other events in a logic diagram. The term "logical constants" refers to gates. The names, "events" and "gates", are terms more commonly used in system safety and are retained here. The analyst should realize, however, that "event" and "gate" have the same properties and obey the same laws as "proposition" and "logical constant" defined in symbolic logic. Furthermore, "event" and "gate" can also be thought of as "set" and "operator", respectively, since they have the same properties and obey the same laws as in set theory.

The term "event" denotes a dynamic change of state which takes place in a system element; the term "element" includes hardware, environment, software, personnel, activity, and/or operation. For logic diagrams, the event occurs in either of two states: true or false. When an event is in a true state, it implies the event has occurred, is occurring, or is "on" for a significant duration. Similarly, when an event is in a false state, it has not occurred or is "off". Frequently, the states of an event are also represented by either "1" and "0" or "on" and "off", for true and false, respectively. Thus, every event has a binary nature.

Each event also has two types: failure event and normal event. If the change of state is such that the intended function of the particular element is not achieved, or an unintended function is achieved, the event is an abnormal function or FAILURE EVENT. If the change of state is such that the intended function occurs as planned (or designed), the event is then a normal system function or NORMAL EVENT.

Failure events can be divided into two categories: basic events and gate events. The basic event is the dynamic change of state of a single system element from an unfailed state to a failed state. Basic events are related to specific failure rates and duration times. These events are used only as inputs to a logic gate (never as outputs) and are, therefore, independent events. A basic event is depicted on the logic diagram by a circle.

The gate event is the resultant output event of a logic gate, dependent upon the type of logic gate. Therefore, the gate event is a dependent event. It must be noted that this event is not the logic gate itself, but the output of the logic gate. The gate event is related to failure rate and duration time, which, in turn, depend upon the input events and the type of logic gate. As development progresses, gate events on one level become inputs to gate events on the next higher level. This gate event is also called a COMMAND EVENT.

The normal event is the expected or desired change of state of a system element. A rate of occurrence and an event duration time are associated with this event. The normal event is used only as an input to a logic gate (never as an output) and is, therefore, an independent event.

A gate denotes a relationship of the state of one event to the state of one or more other events. The basic gates used in a logic diagram are "OR" and "AND". If OR and AND are considered as basic, then all other gates can be resolved into these two.

A summary of the most common symbols used by logic diagram analysts is shown in Figure D-1. The various event and gate symbols are in the first column, the use is explained in the second.

Logic Diagram Structuring

Basically a logic diagram is built by constructing one or more segments, each consisting of an output event, preceded by a logical implication represented by a combination of the symbols shown in Figure D-1. These symbols depict a cause-effect relation to the output event as shown in Figure D-2.

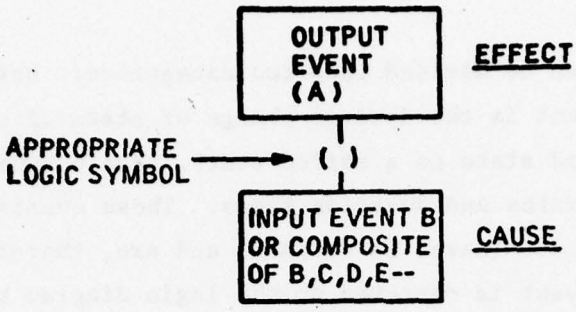


FIGURE D-2. ELEMENTARY CAUSE-EFFECT RELATIONSHIP

If output event (A) is the top event under study, and input event B is the type that can be identified by a circle, a house, or a diamond, then the tree is completed and has one segment consisting of three elements (two events and a logic symbol). If the input event is a composite of events B, C, D, E, etc. where each input event is identified by a circle, a house, or a diamond, the tree is completed and has one segment, made up of two elements more than the number of composite input events.

If one or more of the input events cannot be identified with a circle, house, or diamond, and is identified by a rectangle, then any such event becomes the output event (gate event or command event) of a new segment which must be developed. The diagram continues in this manner until all originating input events are identified by circles, diamonds, or houses.

To clarify the above discussion, assume that top event A of Figure D-3 is to be analyzed. Upon analyzing event A, it is determined there are four input events, A11, A12, A13, and A14, and any one or any combination of all (OR gate) can cause event A to occur. Further examining these events, it is found that event A11 is a primary failure mode of a component, identified by a circle (refer to Figure D-1) and event A12 is an external energy source (not intended by the design) which could cause A to occur. This is a secondary failure mode and can be identified by a diamond. Events A13 and A14 are failure modes which can be caused by other events from a subsystem or components downstream, and are gate or command events which are identified by rectangles. Thus, the first segment (sometimes called first level) of a logic diagram is completed as shown in that part of Figure D-3 which lies above the heavy line.

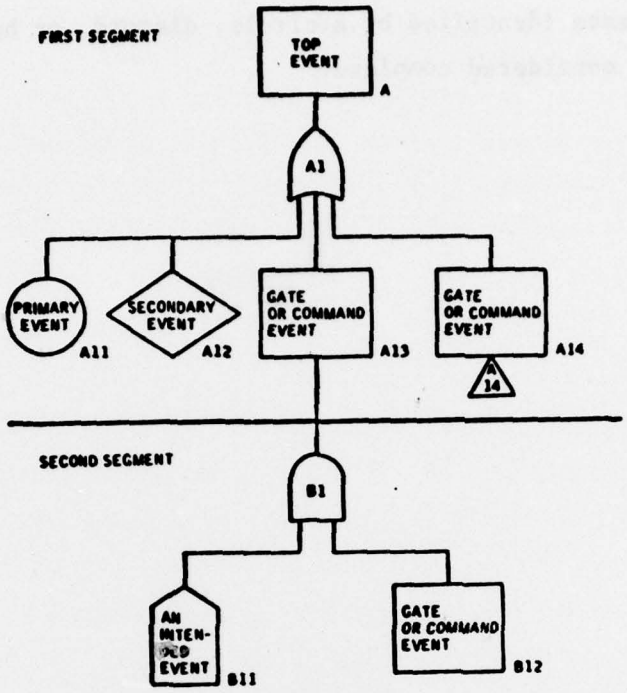


FIGURE D-3. FAULT-TREE SEGMENTS

Since A13 and A14 affect state of the system, they will require further analysis. If because of space or information limitations it is decided that event A14 will be transferred to another page or analyzed at a later date, the transfer gate is used, as indicated. Event A13 is analyzed considering what other event or events are immediately necessary and sufficient to create event A13. To meet the immediately necessary and sufficient requirements, two events, B11 and B12, must occur simultaneously to produce event A13. In this case, an AND gate connecting B11 and B12 is required. Furthermore, event B11 is a normally expected function, not a failure, and should be identified by a house. B12 is identified as a gate event and needs to be further analyzed. From this information, a second segment consisting of A13 as the output and B11 and B12 as the composite inputs defined by an "AND" gate is shown by the section of Figure D-3 lying below the heavy line. Now B12 becomes the command or top event. Following the same reasoning as outlined, another segment of the tree is constructed. Repeat this procedure until no further command events can be identified. When all input

events are independent events identified by a circle, diamond, or house, the logic diagram analysis is considered complete.