REPORT NO. C[illegible]-47-82

RELIABILITY ANALYSIS OF LARGE COMMERCIAL VESSEL ENGINE ROOM AUTOMATION SYSTEMS

VOLUME I

RESULTS

C.E. DAVIS
W.C. GRAHAM

DOVAP & ASSOCIATES
427 Manchester Avenue
Playa del Rey, CA 90291

NOVEMBER 1982

PREPARED FOR

U.S. DEPARTMENT OF TRANSPORTATION
UNITED STATES COAST GUARD
OFFICE OF RESEARCH AND DEVELOPMENT
WASHINGTON, D.C. 20590

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
CG-D-47-82	AD-A135497	

4. Title and Subtitle
Reliability Analysis of Large Commercial Vessel Engine Room Automation Systems Volume I - Results

5. Report Date
November, 1982

6. Performing Organization Code

8. Performing Organization Report No.

7. Author(s)
C.E. Davis and W.C. Graham

9. Performing Organization Name and Address
DOVAP & ASSOCIATES
472 Manchester Avenue
Playa del Rey, CA 90291

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DTCG23-81-20005

13. Type of Report and Period Covered
Final Report
July 1981 - Nov. 1982

12. Sponsoring Agency Name and Address
U.S. Department of Transportation
United States Coast Guard
Office Research and Development
Washington, D.C. 20590

14. Sponsoring Agency Code
G-DMT-1

15. Supplementary Notes

16. Abstract

This report documents a reliability study of large (1,600 tons and over) commercial vessel engine room automation systems. The total effort involved conducting a literature search on maritime automation and reliability topics, analyzing the engine room automations systems on two steam vessels and one diesel vessel, conducting a criticality evaluation, preparing reliability-related design and performance criteria, and evaluating reliability aspects of preventative maintenance.

For the vessels evaluated, Failure Modes and Effect Analyses (FMEA'S) were conducted and fault trees developed. Reliability predictions were computed at several levels of hardware grouping. The criticality impact of potential failure effects was investigated in terms of time constraints and failure detection provisions. A number of recommendations are offered for improving the reliability of current and future engine room automation systems.

This is Volume I of three (3) volumes. Volume II contains Appendices A through C and Volume III contains Appendices D through G.

17. Key Words	18. Distribution Statement
Reliability Vessels (Commercial) Automation Systems Engine Room FMEA'S	Document is available to the U.S. public through the National Technical Information Service, Springfield, VA 22161

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) Reproduction of completed page authorized

PREFACE

This report describes a reliability analysis of large (1,600 tons and over) commercial vessel engine room automation systems. The work was performed by DOVAP and Associates for Headquarters, U.S. Coast Guard, under Contract DTCG23-81-C20005.

U.S. Coast Guard Technical Monitors were Dr. C.P. Chuang and LTJG K.A. Nugent, USCG.

The authors wish to express their gratitude for the excellent cooperation received from the many firms and individuals involved in this study. This includes the ship owners, operators, and crews, and the automation system manufacturers, repair firms, and hardware suppliers. In all cases, DOVAP's requests for information and documentation were granted.

Members of the DOVAP study team were C.E. Davis, W.C. Graham, D. Harris, P. Henmi, J. Medland, P. Nicholson, Dr. L. Phillipson, G. Resnick, and W. Severson. In addition, the authors wish to acknowledge the efforts of M. Jones, K. Parsons, C. Range, and M. Csiszer for their assistance in report preparation.

METRIC CONVERSION FACTORS

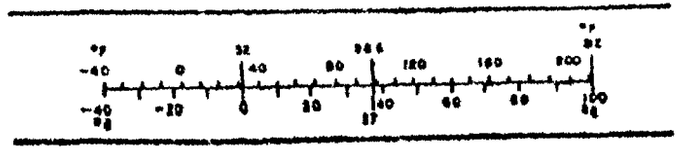
Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
in	inches	*2.8	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
		AREA		
in^2	square inches	6.5	square centimeters	cm^2
ft^2	square feet	0.09	square meters	m^2
yd^2	square yards	0.8	square meters	m^2
mi^2	square miles	2.6	square kilometers	km^2
	acres	0.4	hectares	ha
		MASS (weight)		
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
		VOLUME		
tsp	teaspoons	5	milliliters	ml
Tbsp	tablespoons	15	milliliters	ml
fl oz	fluid ounces	30	milliliters	ml
c	cups	0.24	liters	l
pt	pints	0.47	liters	l
qt	quarts	0.95	liters	l
gal	gallons	3.8	liters	l
ft^3	cubic feet	0.03	cubic meters	m^3
yd^3	cubic yards	0.76	cubic meters	m^3
		TEMPERATURE (exact)		
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C

*1 in = 2.54 (exactly). For other exact conversions and more detailed tables, see NBS Misc. Publ. 286, Units of Weights and Measures, Price $2.25, SD Catalog No. C13.10:286.

Approximate Conversions from Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
		LENGTH		
mm	millimeters	0.04	inches	in
cm	centimeters	0.4	inches	in
m	meters	3.3	feet	ft
m	meters	1.1	yards	yd
km	kilometers	0.6	miles	mi
		AREA		
cm^2	square centimeters	0.16	square inches	in^2
m^2	square meters	1.2	square yards	yd^2
km^2	square kilometers	0.4	square miles	mi^2
ha	hectares (10,000 m^2)	2.5	acres	
		MASS (weight)		
g	grams	0.035	ounces	oz
kg	kilograms	2.2	pounds	lb
t	tonnes (1000 kg)	1.1	short tons	
		VOLUME		
ml	milliliters	0.03	fluid ounces	fl oz
l	liters	2.1	pints	pt
l	liters	1.06	quarts	qt
l	liters	0.26	gallons	gal
m^3	cubic meters	35	cubic feet	ft^3
m^3	cubic meters	1.3	cubic yards	yd^3
		TEMPERATURE (exact)		
°C	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°F



I. EXECUTIVE SUMMARY

This report documents a study of the reliability of large (over 1,600 tons) commercial vessel engine room automation systems. The overall objective of the study was to provide the U.S. Coast Guard with quantitative and qualitative information for use in assessing potential relationships between engine room automation system reliability and vessel navigation safety hazards.

Task I of this study consisted of a search and review of the open literature. The effort focussed on marine automation systems and their reliability and maintainability characteristics. Over 250 documents were reviewed, from which 115 were deemed applicable to the study. The general conclusions reached from the literature review are as follows:

a) The reliability of commercial vessel automated propulsion systems needs improvements;

b) No formal reliability efforts related to design are currently applied by United States manufacturers;

c) When discussing individual problem areas, most papers state that sensors are problems but give no positive suggestions for improvement;

d) Components are selected primarily on the basis of cost, unless component provisions are specifically stated in the design criteria;

e) It is generally agreed that automated propulsion systems for commercial vessels should be better supported with improved training, improved manuals and documentation, and better spares and preventative maintenance programs;

f) Standard environmental criteria needs to be defined and;

g) A commercial vessel failure data system needs to be established.

In reviewing all literature sources, certain subjects were conspicuous by their absence. These are:

a) No formal reliability evaluations of commercial vessel systems were reported.

b) No cost effectiveness studies of current propulsion systems were reported.

The major part of Task II consisted of a reliability analysis of three typical vessels. These included two steam vessels, and one diesel. The reliability analysis included reliability predictions, failure modes and effects analyses (FMEA), criticality analysis, and fault tree analyses. For the failure rate predictions, five categories of rates were generated. These are:

a) Basic failure rates.

b) Failure rates which would be experienced from higher ambient temperatures.

c) Failure rates which would be experienced with better quality parts.

d) Failure rates which would be encountered during the vessels' premature (or initial) period.

e) Failure rates which results from ideal maintenance practices.

The overall basic failure rate predictions for the automated engine room controls for the three ships are as follows:

	Basic Failure Rate (Failure per Hours)	Mean Time Between Failure
Ship A (Steam)	.007988	125.2 hours
Ship B (Steam)	.003622	276.1 hours
Ship C (Diesel)	.001015	984.9 hours

The highest predicted failure rate for the three systems evaluated is for Ship A, which averages approximately 5.8 predicted failures per month. It is predicted that Ship B will average approximately 2.6 failures per month. The principal reason for the difference between the two steam vessels is that Ship A's automated propulsion system is more complex than Ship

B's, and Ship A contains a great deal of pneumatic controls which have higher failure rates than electronic controls. Ship C is the diesel vessel and its control system is not comparable to those of the steam systems, which are much more complicated.

Reviews of historical Navy data show a failure rate for their automated engine room control systems of 1.6 failures per month. It was predicted that the commercial vessel failure rates can be reduced by approximately 50 percent through a comprehensive preventative maintenance program. If this were instituted and the basic failure rates were reduced by half, the expected number of failures per month for Ship B would then be 1.3. This prediction of 1.3 failures per month is close to the 1.6 failures per month derived from the Navy's 3M data system for the actual occurrence of Navy propulsion system failures. This gives a relatively good correlation to the predicted values, since the Navy does have a comprehensive preventative maintenance program.

The predicted effect upon the system failure rates due to the other factors are as follows:

a) Increasing the operating temperature from 35 to 50 degrees C. would increase the basic failure rates by 22 percent.

b) Improving the control system quality by using military grade parts would decrease the basic failure rates by 53 percent.

c) The premature failure rates during the first six months of a vessels operation is approximately six times higher than during the remainder of the ships operational life.

The predicted number of failures does not give the actual relationship between reliability problems and potential navigation safety hazards. In order to better evaluate the effects of failures, Failure Modes and Effects Analysis (FMEA), Criticality Analysis and Fault Tree Analysis were performed.

In performing the FMEA's for the three vessels, each part or groups of parts in the automated control systems was analyzed to determine its failure modes, and how the modes effect the subsystem and the system. The results of the FMEA was then used in the quantitative criticality analysis and the fault tree analysis.

Due to the complexity of the criticality analysis and the fact that the basic results would be the same for Ships A and B (the steam vessels), only Ship B was used for the quantitative computer generated criticality analysis. The total predicted failure rate for Ship B, using the basic rates, was 0.003622 failures per hour, or a mean time between failure of 276.1 hours. Using a normal cruising time of 710 hours, the expected number of failures per cruise is 2.57. This data was analyzed using a computerized technique, and Table ES-1 shows the distribution of the 2.57 failures arranged in order of mission criticality. These are predicted frequencies for normal cruising.

During the normal cruising period, permanent damage to either the boiler or turbine is ranked first in terms of criticality. The most frequent mission effect is "small performance degradation," which accounts for 23 percent of the total failures. Because "small performance degradation" is rather inconsequential during normal cruising, the mission loss probability is computed as 0.1. Therefore, even though the classification of the mission effect of "small performance degradation" is highest by frequency, because of the low mission loss probability it is ranked fifth in terms of its contribution to mission criticality.

The computer-generated criticality analysis was validated by comparing the predicted mission effects to actual historical data. For example, the expected frequency of temporarily reduced RPMs was predicted to be 0.29 per cruise. This gives an expected rate per year of 3.4. This compares almost exactly to one report reviewed during Task I which documents 41 ship-years of history, and reports a slowdown rate of 3.3 per ship-year.

The primary conclusion drawn from the criticality analysis is that the majority of the automated propulsion control system failures do not result in mission critical events because the systems are designed with sufficient backup and alarms.

Fault Tree analysis was performed for selected undesirable events for all three ships. The fault tree analysis probabilities were based on the exponential distribution and are computed for one cruise of one-month duration. Each probability of occurrence was computed twice, once with the probability of manual intervention being effective 90 percent of the time (or, noneffective 10 percent of the time), and once with no manual intervention. Noneffective manual intervention could be due to an alarm failure, incorrect action taken by the crew, action not timely enough to prevent problems, etc. The results of the fault tree analysis for ships A and B are summarized in Table ES-2.

MISSION EFFECT CRITICALITY

MISSION EFFECT	SYSTEM EFFECT FAILURE PROBABILITY	PCT. OF SYSTEM FAILURE PROBABILITY	MISSION LOSS PROBABILITY	MISSION CRITICALITY	PERCENT CONTRIBUTION TO MISSION CRITICALITY
POSSIBLE BLR/TURB DAMAGE	.4806	10.53	.5000	.2364	35.44
TEMPORARY LOSS OF RPM CONTROL	.2475	9.540	.6000	.1437	21.52
TEMPORARY REDUCED RPMS	.2891	11.16	.4000	.1147	17.19
TEMPORARY DIW	.9220E-01	3.554	.7000	.6398E-01	9.584
SMALL PERFORMANCE DEGRADATION	.6034	23.26	.1000	.5951E-01	8.914
TEMP LOSS DIRECTIONAL CONTROL	.4648E-01	1.789	.6000	.2735E-01	4.096
BACK-UP FAILURE	.1095	4.219	.2000	.2173E-01	3.254
NO EFFECT	.2363	8.877	.0	.0	.0
NOT APPLICABLE/NORMAL STEAMING	.4948	19.07	.0	.0	.0

TABLE ES-1

Mission Effect Criticality Summary,
Basic Failure Rates,
Normal Steaming Phase

Abbreviations:
PCT; Percent
BLR; Boiler
TURB; Turbine
DIW; Dead in the Water
TEMP; Temporary

TABLE ES-2

Probability Of Undesirable Events Occuring
Per Cruise (730 Hrs) and
Expected No. Per Year, Ships A and B

	Assuming a 90% Correct Manual Intervention				No Manual Intervention	
	Ship A *	No. Per Year	Ship B *	No. Per Year	Ship A *	Ship B *
1. Unscheduled Turbine Shutdown	0.1584	1.90	0.1065	1.27	0.5186	0.2861
1a Combustion Explosion	0.0180	0.21	0.0143	0.17	0.0297	0.0522
1b Steam Explosion	0.00014	0.002	0.0046	0.055	1.42×10^{-4}	0.0451
1c Single Boiler Trip	0.1244	1.49	0.0446	0.54	0.2040	0.0606
1d Both Boiler Trip Due To A Common Cause	0.0392	0.47	0.004	0.005	0.1986	0.0131
2. Turbine Damage	0.0358	0.42	0.0392	0.47	0.1026	0.1360
3. Loss of Speed/Directional Control	1.1×10^{-6}	-	1.1×10^{-6}	-	-	-
3a Loss of Primary TC**	0.1682	2.02	0.1682	2.02	-	-
3b Loss of Hand Pump	0.0246	0.29	0.0246	0.29	-	-
3c Loss of Handwheel	0.0027	0.03	0.0027	0.03	-	-

(*Probability)
(**Throttle Control)

One of the top undesirable events is unscheduled turbine shutdown. The probability that Ship A will experience an unscheduled turbine shutdown when manual intervention is 90 percent effective during a cruise is predicted to be 0.1584; the probability for Ship B is 0.1065. This amounts to approximately 1.9 such shutdowns per year for Ship A and 1.27 for Ship B. The probabilities increase significantly with no manual intervention; for Ship A the probability increases to 0.5186 and for Ship B to 0.2861.

As a comparison to actual historical data, the 1.9 and 1.27 predicted stoppages at sea are relatively close to those reported in a document that summarizes the stoppage history of 29 tankers. This paper reports an average stoppage at sea rate of one per ship per year.

The predicted probability of explosion, either combustion or steam, is 0.0181 for Ship A and 0.0189 for Ship B. This amounts to an estimated mean time between explosions of 39,000 hours for Ship A and 37,000 for Ship B. As a comparison, it was estimated from two sources of historical data that explosions occur once every 36,000 hours in steam systems. Therefore, the estimates for Ship A and Ship B are relatively close to the estimates generated from historical analysis.

The probability of the top undesirable event of "loss of speed/directional control" for the steam vessels becomes inconsequential due to redundancy. The likelihood of loss of the primary throttle control mode, with a probability of 0.1682 per cruise, is relatively high. However, double redundancy is provided by the hand pump and the hand wheels, so probability of losing all control modes becomes extremely small.

The top event for the diesel system fault tree is "vessel does not respond as commanded due to engine room automation faults." The probability of this top event is 0.072, or roughly 0.9 occurrences per year.

Based on the predicted values and the data from the literature search, it is felt that the automated propulsion systems analyzed during this study have acceptable levels of reliability for the current mode of operation. However, it must be noted that this applies to the conditions considered during the study analyses. If a specific vessel spends a great deal of time maneuvering and in close quarters, the reliability of the propulsion automation system must be substantially higher. With the current level of technology, the reliability of commercial vessel automated propulsion systems could be magnitudes higher. However, most increases in reliability also entail increases in

cost, and there is not a one-to-one ratio between improvements in reliability and relative increases in cost. As increasingly higher levels of reliability are sought, the ratio of cost to reliability increases. Also, increased reliability does not necessarily decrease maintenance costs. On the contrary, increased reliability often results in increased complexity which can have the net effect of increasing maintenance costs.

In order to optimize reliability, maintainability, and costs of any new automated propulsion system, it is recommended that early in the design stage all requirements of proposed systems be predefined and cost trade-offs considered. A system specification should be generated jointly by the control system manufacturer, the shipyard, and the owner/operator. The system specification should call-out the desired levels of reliability for critical functions, and specify how the desired levels are to be achieved. The system specification should also define how the system is to be supported during its operational life.

In the area of operational support, the system specification should specify the type and extent of training required for the various crew members, and required levels of manning. If periods of unmanned engine room operation are planned, alarm provisions should be adequate, and certain critical alarms should be redundant. The systems specification should also delineate how the engine room is to be manned during the first 6 months of operation when failure rates could be up to six times greater than during the steady state period of the operational life. Additionally, the system specification should contain provisions for minimizing the problems incurred during this initial period; this should include workmanship requirements to reduce manufacturing-induced problems, and through requirements for system tests to be conducted at the shipyard and during sea trials. The system specifications should also describe in detail the preventative maintenance plan that will be applied during the operational life of the system, including how components which are subject to degradation or wearout are to be periodically replaced or overhauled.

It is recommended that a data system for the collection of failure related information be established in order to reduce subjective biases, and provide objective means for evaluating costs, components failure rates, maintenance and approaches, and other reliability-related factors.

TABLE OF CONTENTS

Section Number		Page Number
I	INTRODUCTION.	I- 1
	A. Study Objective and Tasks.	I- 2
	B. Study Approach and Report Organization. . . .	I- 4
II	THE FUNDAMENTALS OF RELIABILITY	II- 1
	A. The Theoretical Basis of Reliability	II- 1
	B. The Probabilistic Nature of Reliability Predictions.	II- 3
	C. Failure Rates.	II- 3
	D. Reliability Implications of Time	II- 4
	E. Reliability Implications of the Number of Parts.	II- 5
	F. Redundancy and Reliability Modelling	II- 5
	G. Reliability Block Diagrams	II- 8
	H. Reliability Implications of Part Failure Rates.	II-10
	I. Failure Modes and Effects Analyses	II-13
III	GENERAL DISCUSSION OF CONTROL SYSTEMS	III- 1
	A. Steam Turbine Control Systems.	III- 1
	.(1) Boiler Control	
	.(2) Turbine Controls	
	.(3) Auxiliary Control	
	B. Diesel Vessel Control Systems.	III- 4
IV	LITERATURE REVIEW	IV- 1
	A. Literature Search Approach	IV- 1
	.(1) Abstract and Title Search	
	.(2) Document Acquistion and Review	
	.(3) Summarization and Cross-Referencing	
	B. Literature Search Findings and Conclusions .	IV- 4
	.(1) R&M Quantitative Data	
	.(2) R&M Qualitative Data	
	.(3) Maritime R&M Status Information	
	.(4) Automation Configuration Information	
	.(5) Automation State-of-the-Art	
	.(6) Spare Parts Assessments	
	.(7) Regulations/Requirements	
	.(8) Environmental Information	
	.(9) Other	

TABLE OF CONTENTS

Section Number		Page Number
V	CONTROL SYSTEMS SELECTED FOR STUDY.	V- 1
	A. Control Systems Selection Process.	V- 1
	B. Ship A Characteristics, Coverage and Ground Rules	V- 2
	.(1) Ship A Characteristics	
	.(2) Ship A Boiler and Combustion Control Characteristics	
	.(3) Ship A Turbine Speed Direction Control Characteristics	
	.(4) Ship A Coverage and Ground Rules	
	C. Ship B Characteristics, Coverage and Ground Rules	V- 6
	.(1) Ship B Characteristics	
	.(2) Ship B Control System Characteristics	
	.(3) Ship B Coverage and Ground Rules	
	D. Ship C Characteristics, Coverage and Ground Rules	V- 8
	.(1) Ship C Characteristics	
	.(2) Ship C Coverage and Ground Rules	
VI	FAILURE RATE PREDICTIONS.	VI- 1
	A. Failure Rate Sources	VI- 1
	B. Development of Failure Rates for Commercial Vessel Automated Controls.	VI- 4
	.(1) Environmental K-Factors For Non-Electronic Parts	
	.(2) Development of Part Class and Type Failure Rates For Commercial Vessel Control Room Application	
	.(3) Adjustment Factors For Reducing Basic Failure Rates Through Functional Testing, Inspection, And Scheduled Maintenance	
	.(4) Adjustment Factors For "Opens" From The Field	
	.(5) Substantiation of Six Month Factors For Hardware Other Than Electronic Components	
	C. Electronic Parts Stress Analysis	VI-10
	D. Reliability Growth and the Effect of Screened and Unscreened Circuit Cards. . . .	VI-11
	E. Electronic Part Failure Rate Generation. . .	VI-13
	.(1) Application of MIL-Handbook 217	
	.(2) Analysis Of The Effect Of Temperature	
	.(3) The Effects Of Higher Quality Levels	
	.(4) Failure Rate Summary	

TABLE OF CONTENTS

Section Number		Page Number
VII	FAILURE MODES AND EFFECTS ANALYSIS (FMEA) . . .	VII- 1
	A. FMEA Approach.	VII- 1
	B. Failure Modes.	VII- 3
	C. FMEA Example	VII- 5
	D. FMEA Points of Interest.	VII-10
	.(1) FMEA Realism	
	.(2) FMEA Comparability	
VIII	FAULT TREE ANALYSIS	VIII- 1
	A. General Discussion	VIII- 1
	.(1) Primary Events	
	.(2) Intermediate Events	
	.(3) Gates	
	.(4) Transfers Within The Fault Tree	
	.(5) Construction Rules	
	B. Quantitative Fault Tree Analysis Through Boolean Algebra.	VIII- 6
	.(1) Rules of Boolean Algebra	
	C. Fault Tree Models and Assumptions.	VIII- 7
	D. Points of Interest	VIII-10
	.(1) General	
	.(2) Quantitative Points of Interest	
IX	CRITICALITY ANALYSIS.	IX- 1
	A. General Criticality Analysis	IX- 1
	B. Quantitative Criticality Analysis.	IX- 4
	.(1) Factors Impacting Criticality	
	C. Quantitative Criticality Analysis Procedure.	IX-10
	.(1) Grouping of Failure Modes	
	.(2) Criticality Analysis Summary Sheets	
	.(3) Systems Effects Summary	
	.(4) Mission Criticality	
	.(5) Quantitative Criticality Computer Analysis	

TABLE OF CONTENTS

Section Number		Page Number
X	RELIABILITY DESIGN AND PERFORMANCE CRITERIA . .	X- 1
	A. Design and Performance Criteria Basic Overall Requirement.	X- 1
	B. The Causes of Unreliability.	X- 2
	.(1) Infant Mortality Failures	
	.(2) Wearout Failures	
	.(3) Steady State Failures	
	.(4) System Downtime	
	C. Reliability Design and Performance Criteria.	X- 6
	.(1) Reliability Improvement Categories	
	.(2) Downtime Reduction Categories	
XI	MAINTENANCE ANALYSIS.	XI- 1
	A. Background and Historical Data	XI- 1
	B. Logistics Support Analysis Program	XI- 2
	C. Maintenance Analysis Approach.	XI- 6
	D. Preventative Maintenance Analysis.	XI- 6
	.(1) State-Of-The-Art Of Preventative Maintenance	
	.(2) Steam Control System Preventative Maintenance	
	.(3) Diesel Control System Preventative Maintenance	
XII	MISCELLANEOUS STUDY OBSERVATIONS	XII- 1
	A. Environmental Consistency	XII- 1
	B. Atomizing Steam Source.	XII- 2
	C. Technology Approach	XII- 2
	D. Operational Approach	XII- 4
	E. Fault Trees vs. FMEA's.	XII- 4
	F. Wiring.	XII- 6
XIII	GUIDELINES FOR COAST GUARD USE	XIII- 1
	A. Design Approval Guidelines.	XIII- 1
	.(1) Suggested Systems Specifications Outline	
	B. Accident Investigation Guidelines	XIII- 8
	C. Inspection and Test Guidelines.	XIII-10
	.(1) Steam Vessel Considerations	
	.(2) Diesel Vessel Inspection Considerations	
	D. Guidelines for Crew Training and Experience Considerations.	XIII-22
	..(1) Training and Experience Factors	
	.(2) Automation Personnel	
	.(3) Additional Comments	

TABLE OF CONTENTS

Section Number		Page Number
XIV	CONCLUSIONS AND RECOMMENDATIONS.	XIV- 1
	A. Results of Predictions.	XIV- 3
	B. Failure Modes and Effects Analysis.	XIV- 4
	C. Criticality Analysis.	XIV- 5
	D. Fault Tree Analysis	XIV- 7
	E. Overall Conclusions and Recommendations . . .	XIV-10

Appendices

A	TASK I LITERATURE SEARCH	A- I
B	SHIP A FMEA.	B- 1
C	SHIP B FMEA.	C- 1
D	SHIP C FMEA.	D- 1
E	FAULT TREES.	E- 1
F	CRITICALITY ANALYSIS SUMMARY SHEETS.	F- 1
G	PREDICTOR CRITICALITY PRINT-OUTS	G- 1

LIST OF TABLES

Number		Page Number
I- 1	Probability of Undesirable Events Occurring. .	I- 4
II-1	Part Failure Rate.	II-13
IV- 1	Average Number of Alarms per Month	IV- 8
IV- 2	Reported Faults Resulting in Main Boiler Auto-Shutdown.	IV-10
IV- 3	Reported Faults Inhibiting the Relighting of the Burners (Log #097)	IV-10
IV- 4	Reported Faults that Could Have Resulted in the Loss of Propulsion (Log #097).	IV-12
IV- 5	Total Number of Incidents by System Excluding Failures Not Related to Current Study (Log #097)	IV-13
IV- 6	Types of Faults (Log #097)	IV-14
IV- 7	Operational Vessel Failure Summary (Log #083).	IV-15

LIST OF TABLES

Number		Page Number
IV- 8	Failure Effect Data (Log #066)	IV-17
IV- 9	Relationship of Initial Failure Rate Period to Random Failure Rate Period and Major Contributions (Log #075)	IV-18
IV-10	Log #508, ARINC Report; Boiler Failures Based 3M Data; Mean Time Between Failure, Forced Shutdown.	IV-20
IV-11	Accidents Reported by National Board Members and Other Authorized Inspection Agencies. . . .	IV-20
IV-12	Ships Covered in 3M Special Data Run.	IV-22
IV-13	Summary of Data from Navy Maintenance Material Management System	IV-23
IV-14	Environmental Specifications.	IV-29
VI- 1	K-Factor Development for Non-Electronic Parts, Factors for Converting Other Environments to Ship Sheltered.	VI- 6
VI- 2	Commercial Vessel Failure Rate Development for Non-Electronic Parts.	VI- 7
VI- 3	Failure Rate Factor Summary Table	VI-26
VII- 1	Ship A Subsystem Breakdown.	VII-13
VII- 2	Ship B Subsystem Breakdown.	VII-14
VII- 3	Ship C Subsystem Breakdown.	VII-15
IX- 1	Summary of How Factors Change the Frequency of System Effects--Normal Cruising Phase. . . .	IX-44
XIII- 1	Recommended Priorities for Operational Tests of the Automation Systems for Steam Turbine Systems	XIII-12
XIV- 1	Probability of Undesirable Events Occurring Probabilities per Cruise (730 Hours) and Expected Number per Year, Ships A and B	XIV- 8

LIST OF FIGURES

Number		Page Number
I- 1	Mission Effect Summary, Basic Failure Rates, Normal Steaming Phase.	I- 6
IV- 1	Number of True Alarms.	IV- 7
VI- 1	Example of Component Stress Ratio and Temperature Rise Worksheet	VI-12
VI- 2	Reliability Growth of Electronic Equipment .	VI-14
VI- 3	Sample Group of Electronic Parts (Failure rates calculated using MIL Handbook 217 methods, naval sheltered environment, ambient temperature of 35 degrees C. and lower military grade quality).	VI-15
VI- 4	Sample Group of Electronic Parts (Failure rates calculated using MIL Handbook 217 methods, naval sheltered environment, ambient temperature of 35 degrees C. and commercial grade quality)	VI-19
VI- 5	Sample Group of Electronic Parts (Failure rates calculated using MIL Handbook 217 methods, naval sheltered environment, ambient temperature of 50 degrees C. and commercial grade quality)	VI-22
VII- 1	Simplified Schematic of Logic Covered in FMEA Sample Sheets	VII- 6
VII- 2	Sample of FMEA Worksheets.	VII- 7
IX- 1	Typical Criticality Sheet.	IX-12
IX- 2	System Criticality for Maneuvering	IX-21
IX- 3	Mission Criticality for Maneuvering.	IX-21
IX- 4	System Criticality for Light-Off	IX-22
IX- 5	Mission Criticality for Light-Off.	IX-22
IX- 6	System Criticality for Normal Steaming . . .	IX-23
IX- 6A	Mission Criticality for Normal Steaming. . .	IX-23
IX- 7	Input Data for Computer Criticality Analysis, Ship B	IX-24

LIST OF FIGURES

Number		Page Number
IX-8	System Effects, Basic Failure Rate and Normal Steaming Phase.	IX-35
IX-9	System Effects, Temperature Increased to 50° C., Normal Steaming Phase.	IX-35
IX-10	System Effects, Quality Increased to Lower Military Grade, Normal Steaming Phase. . . .	IX-36
IX-11	System Effects, Premature Failure Rates Used, Normal Steaming Phase.	IX-36
IX-12	System Effects, Basic Rates Reduced as Results of Comprehensive Preventative Maintenance, Normal Steaming Phase	IX-37
IX-13	Contribution of Each Subsystem to Individual Mission Effect	IX-40
X- 1	Excessive Interface Parts.	X- 8
X- 2	Excessive Signal Conditioning.	X- 8
X- 3	Printed Circuit Card Filter Capacitors . . .	X-18
X- 4	Relay Arc Suppression Diodes	X-19
X- 5	Alternate Implementations of the Same Logic Functions.	X-29
XI- 1	Cumulative Ship Availability by Quarter After Overhaul	XI- 3
XI- 2	Problem Reporting Frequency.	XI- 4
XIV- 1	Mission Effect Summary, Basic Failure Rates, Normal Steaming Phase.	XIV- 6

LIST OF ABBREVIATIONS

ABS	American Bureau of Shipping
A/D	Analog to Digital
AH	Ahead
AIF	Aircraft Inhabited Fighter
AIT	Aircraft Inhabited Transport
APL	American President Lines
A/R	Air Register
AS	Astern
AUT	Aircraft Uninhabited Transport
BCD	Binary Coded Decimal
Blr	Boiler
Bnr	Burner
Br	Bridge
C.A.	Combustion Air
C.E.O.	Chief Engineering Officer
C.P.	Controllable Pitch
CPU	Central Processing Unit
CPP	Controllable Pitch Propeller
CRP	Controllable, Reversible Pitch Propeller
D.G.	Diesel Generator
D.O.	Diesel Oil
DWT	Dead Weight Tons
ECR	Engine Control Room
EMI	Electromagnetic Interference
EOT	Engine Order Telegraph
E/P	Electro/Pneumatic
ER	Engine Room
ERC	Engine Room Console
ESD	Electrostatic Discharge
FDB	Forced Draft Blower
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
F.O.	Fuel Oil
F.P.	Feed Pump
F.W.	Feed Water
FY	Fiscal Year
GIDEP	Government/Industry Data Exchange Program
GRT	Gross Rated Tons
hp	Horsepower
H.P.	High Pressure

IEEE	Institute of Electrical and Electronic Engineers
IMCO	Inter-Governmental Maritime Consultative Organization (now IMO)
IMO	International Maritime Organization (formerly IMCO)
ITC	Integrated Throttle Control
J.W.	Jacket Water
LED	Light Emitting Diode
LNG	Liquified Natural Gas
L.O.	Lube Oil
L.P.	Low Pressure
L.V.D.T.	Linear Variable Differential Tranformer
MarAd	Maritime Administration
M&R	Maintenance and Repair
MI	Mechanical Idle
MPC	Malfunction Proportional Control
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
MUX	Multiplexer
MV	Motor Vessel
N.C.	Normally Closed
N.O.	Normally Open
NTSB	National Transportation Safety Board
NUC	Nuclear Power Plant
P.B.	Pushbutton
P.C.	Printed Circuit
P/D	Propeller Actual Pitch to Diameter Ratio
P.I.	Pneumatic Idle
PM	Preventative Maintenance
QMED	Qualified Member of the Engineering Department
RAY	Raytheon
R&D	Research and Development
R&M	Reliability and Maintainability
RCM	Reliability Centered Maintenance
RTD	Resistance Temperature Detector
SDG	Shaft Driven Generator
S.H.	Superheated
SHP	Shaft Horsepower
SNAME	Society of Naval Architects and Marine Engineers
SOLAS	Safety of Life at Sea
SPDT	Single Pole Double Throw

SPST	Single Pole Single Throw
SRC	Slew Rate Controller
SS	Steamship
S.W.	Salt Water
TACH	Tachometer
TC	Throttle Control
T.G.	Turbo-Generator
TT	Turbine Tanker
ULCC	Ultralarge Crude Carrier
UMS	Unattended Machinery Spaces
USCG	United States Coast Guard
VLCC	Very Large Crude Carrier
Vlv	Valve
WET	Environment is Wet

I. INTRODUCTION

Due to the rising costs of labor, fuel and insurance, and to the need for higher reliability and safety, it is evident that certain types of automated engine room controls are necessary in order for vessel operations to maintain a competitive position in the marine industry. The problem faced by ship owners/operators is to determine the degree to which automation should be employed, and the type of equipment that should be used to minimize life cycle costs and maximize reliability and safety. The Coast Guard also is concerned since unreliable automated engine room systems could be causes or major contributing factors to vessel casualties. Thus, the Coast Guard contracted with DOVAP and Associates to conduct a study of engine room automation systems. The overall purpose of the study was to evaluate the reliability of current engine room control systems, and to provide information and insights as to how future systems could be improved.

The study was contractually stipulated to evaluate the reliability of automated engine rooms for commercial vessels over 1600 tons. The automated systems to be evaluated included combustion control systems, feedwater control, flame safeguard control, burner management, throttle control, and alarm systems. Such systems were evaluated for two different steam vessels. In addition, the automated controls were evaluated for one diesel vessel.

Although the study was primarily concerned with the reliability of automated engine room systems, the effect of maintenance was also to be considered, as was the human interface and backup. Besides being designed to replace the human element, the systems perform more efficiently than the human watchstander. But as with any system, there is no such thing as a perfectly designed system which always functions as intended. Therefore, the human interface could not be eliminated from this study.

A. STUDY OBJECTIVE AND TASKS

The overall ob,ective of this study was to provide the U.S. Coast Guard with quantitative and qualitative information for use in assessing potential relationships between engine room automation system reliability and vessel navigation safety hazards. To generate this information, three tasks were contractually stipulated. Additional guidance from the Coast Guard was provided at two workshops held at Coast Guard Headquarters upon completion of Task I, and later Task II.

Task I consisted of a survey of the open literature. The objective of the literature survey was to review all published documents related to the reliability of automated engine room controls. Over 250 documents were reviewed, from which 115 were deemed applicable to the study in some manner.

The objective of Task II was to evaluate the reliability of current, operational automated engine room controls. Task II was originally structured to consist of detailed reliability analyses of two steam vessels and two diesel vessels. Two of the vessels were to be mechanical-based control systems and two were to be computer-based. DOVAP's first effort on this task was to contact a number of owner/operators, shipyards, and automation system manufacturers in order to compile a candidate list of vessels with automated engine rooms. This effort revealed that there were no currently operating, large U.S. flag vessels with computer-based automated engine rooms. Task II was then restructured to consist of evaluations of two steam vessels, one diesel vessel, and a criticality analysis in lieu of analysis of the second diesel vessel.

The detailed analyses of the three vessels included, for each, Failure Modes and Effects Analyses (FMEA), reliability predictions, and fault tree analyses. Three major objectives were established for these analyses of the three vessels. The first was that the systems evaluated represent different technological approaches but current state-of-the-art. To this end, the Coast Guard selected the particular vessels to be analyzed from the candidate list of vessels developed by DOVAP.

The second major objective for the analysis was that each system be evaluated to the same depth of detail. To accomplish this, DOVAP obtained documentation that would permit analysis down to the detailed circuit level on all three systems. This documentation consisted of circuit schematics, parts lists, wiring diagrams, panel layouts, and various types of technical

manuals.

The third major objective for the analysis was to establish reasonable system boundaries, or, in other words, defining where the engine room control system "stopped" and other ship systems "began". The criteria applied in defining these boundaries was based on whether or not the vessel would be fitted-out with the equipment in question if it did NOT have an automated control system. Based on this criteria, support systems such as ship's electrical power and control air were deemed not a part of the systems to be evaluated since they would be provided on-board regardless of whether the engine room was automated. Other areas ruled out by this criteria are atomizing steam, gland steam, pumps (fuel pumps, lube oil pumps, etc.), and valves not specifically required by the automated controls.

The overall objective of Task III was to translate the results, findings, and observations of Tasks I and II into a baseline of reliability-related information suitable for use by the Coast Guard in its various activities. To achieve this overall objective, four subtasks were established, viz;

a) Delineation of design and performance criteria from a reliability standpoint.

b) Performance of a maintenance analysis of ship automation equipment, and identification of the effect maintenance can have in improving reliability.

c) Recommendation of guidelines for Coast Guard use in the following areas:

    1) Design approval of engine room automation systems.

    2) Accident investigation related to engine room automation system failures.

    3) Period

    4) Recommendation of the desired levels of formal training and experience for automated engine room crew members.

B. STUDY APPROACH AND REPORT ORGANIZATION

In the following paragraphs, the approaches taken to the various study tasks are briefly described. These approach paragraphs are organized below according to the report section where more detailed discussions can be found.

Section II; The Fundamentals of Reliability:

It is anticipated that some readers of this report will have had little or no experience in the field of reliability. Therefore, a section was provided giving tutorial discussions on the fundamentals of reliability. For the sake of brevity, the discussions make no attempt at a textbook level of coverage. Rather, they briefly describe the theoretical basis of reliability and some of the more commonly applied reliability practices.

Section III; General Discussion of Control Systems:

It was felt that some readers of this report might possibly not be acquainted with the operation of engine room control systems. A section was therefore provided to briefly discuss those operational aspects.

Section IV; Literature Review:

During the Task I literature review, approximately 250 documents were initially reviewed, and of these 115 were selected as applicable. The approach taken in the selection was to review all documents that pertained to maritime reliability, or to some other aspect of maritime automation that could conceivably impact reliability (state-of-the-art, maintenance practices, operating experience, environmental effects, etc.) Summaries of the applicable documents were prepared, and accessing codes were set-up. Section IV of this report summarizes the results of this effort, and Appendix A contains the document summaries and accessing codes.

Section V; Control Systems Selected for Study:

Considerable effort was devoted to the selection of the control systems that would be investigated during the study. DOVAP generated a list of candidate systems based on the following criteria:

a) The vessel must have an automated propulsion control system.

b) The candidate vessel should have been handed over to the owner/operator within the last five years. This was to ensure that the system is of the current state-of-the-art, and also that there is substantial operating time on the vessel.

c) The vessel is in excess of 1600 DWT.

d) The vessel has been operated beyond the various warranty periods.

e) The vessel is a U.S. flag.

f) The control system is produced by a U.S. manufacturer.

g) Sufficient documentation on the vessel is available for analysis during the study period.

From the candidate lists, the Coast Guard made the final selection of the systems to be evaluated.

Section VI; Failure Rate Predictions:

Failure rate predictions were generated for the three automated engine room control systems under investigation. The approach taken in generating these predictions was to use failure rates from established sources. In many cases adjustment factors had to be developed to account for the commercial engine room environment.

Section VII; Failure Modes and Effects Analysis (FMEA):

The basic, overall approach to the FMEA's for all three ships was first to subdivide the hardware into realistic, manageable groupings. At the "top level," these groupings constitute the subsystems, or major functional areas.

The hardware within each subsystem was then further subdivided by examining the individual hardware elements. Groupings were established based on the subfunctions performed. The failure modes and effects for each part or group of parts was then determined.

Section VIII; Fault Tree Analysis:

Fault tree analyses describe analytically the undesired states of the systems, and all credible ways in which the undesired events can occur.

For the fault trees developed during this study, the top undesirable events were defined in the Statement of Work. Due to the basic differences between diesel and steam systems, the top, undesirable units are somewhat different for the two types of systems.

The approach to, and findings of, the fault tree analyses are described in detail in Section VIII. The individual fault trees for Ships A, B, and C, respectively, are provided in Appendices B, C, and D.

Section IX; Criticality Analysis:

The criticality analysis was based on information from all other analyses as well as on information obtained by DOVAP personnel during trips aboard the two steam vessels. Quantitative analyses were conducted utilizing this information in order to identify and evaluate the interactions, relationships, and ramifications that can impact the severity of failures. This "severity," in turn, relates to the end effect of the failure on the vessel.

The quantitative criticality analysis focussed on identifying the various "scenario" factors that determine whether or not a potentially critical failure effect will indeed have critical consequences. Where these factors and their various ramifications could be quantified, they were included in the

quantitative analysis.

Section X; Reliability Design and Performance Criteria:

The reliability design and performance criteria were developed as a subtask of Task III. During this effort the design and performance aspects were considered from the standpoint of their role in improving reliability and reducing system downtime.

In conducting this subtask, DOVAP evaluated such factors as design practices, operational characteristics, quality provision, etc., that can impact the reliability of engine room automation systems. A number of candidate areas for improving the probability/effect of engine room automation system failures were identified and categorized. These areas are supported by examples taken from the findings and observations of Tasks I and II, and from information obtained from firms specializing in the repair of engine room automation systems.

Section XI; Maintenance Analysis:

The maintenance analysis which was performed during this study on the components of automation systems was not of the classical logistics support analysis type. That is, because of limitations in the scope of work and undefined maintenance concepts and plans, individual components were not evaluated as part of a total integrated program. Frequency and depth of all maintenance actions in many cases are subjected to trade-offs; however, in this study the engine room maintenance could not be optimized because only a portion of the total engine room equipment was evaluated. Although the automated controls are a very important aspect of the ship's machinery, they require a relatively small portion of the overall vessel's preventative maintenance efforts.

Section XII; Miscellaneous Study Observations:

During the course of the study, several observations were made that were either of a general nature or not specifically applicable to any single study task. These observations involve such areas as technology approach to engine room control and various design aspects that can impact operational procedures.

Section XIII; Guidelines for Coast Guard Use:

As part of Task III, the Statement of Work required that DOVAP develop guidelines for use by the Coast Guard in the following areas of its activities:

a) Propulsion automation system design approval.
b) Accident investigations related to propulsion automation systems.
c) Inspections and test of propulsion automation systems.
d) Crew training and experience considerations.

Section XIV; Conclusions and Recommendations:

This section of the report contains the major conclusions and recommendations from all individual tasks and sub-tasks. It also tabulates the major results of the various quantitative evaluations.

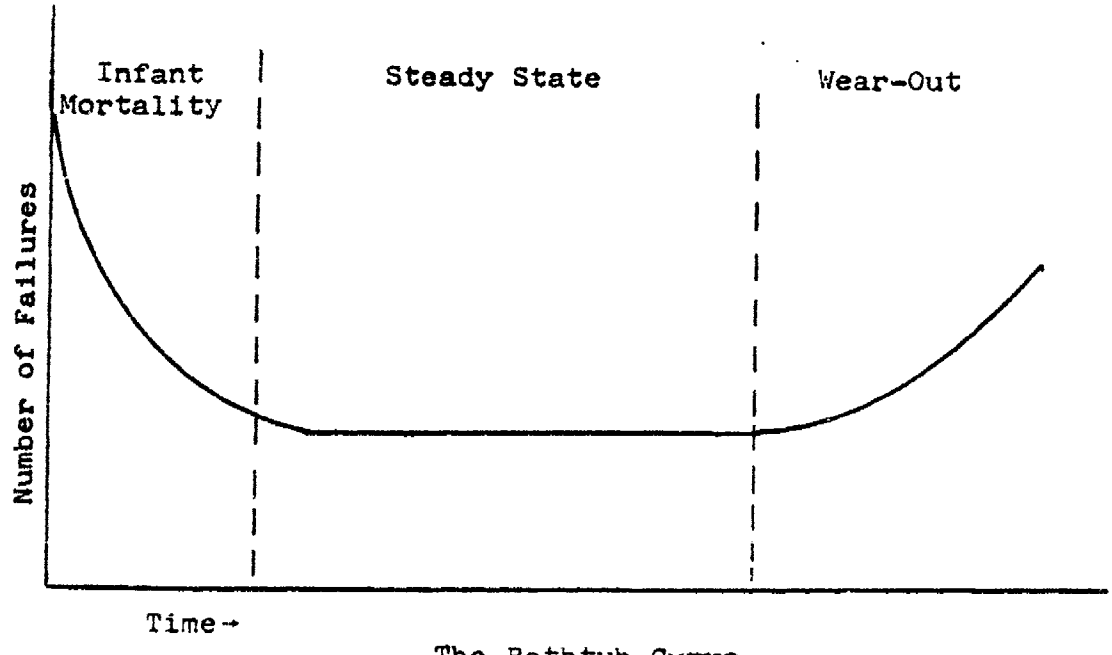
II. THE FUNDAMENTALS OF RELIABILITY

DOVAP expects that some readers of this report will have had little or no experience in the field of reliability. Hence, this section provides tutorial discussions on the fundamentals of reliability so that subsequent report sections can be more readily understood and objectively evaluated. For the sake of brevity, the discussions make no attempt at a textbook level of coverage. Rather, they briefly describe the theoretical basis of reliability and some of the more commonly applied reliability practices.

A. THE THEORETICAL BASIS OF RELIABILITY

The term "reliability" means different things to different people. To some, it implies an intuitive measure of equipment "worth" or "ruggedness"; to others, an indication of dependability. To the reliability analyst, it implies a numerical indication of how "failure prone" an equipment is (or is not). The theoretical basis for such numerical indications of "failure proneness" begins with the bathtub curve.

This curve, as shown below, indicates that infant mortality failures occur early in the life of an equipment, and that after they have been eliminated during the de-bugging process, a period of steady state operation follows. During the steady state, failures occur at their lowest rate. At the onset of equipment wear-out, the number of failures begins to increase, and increases steadily as the aging process continues.



The Bathtub Curve

The statistical implications of the bathtub curve make it far more than simply a common sense observation of equipment failure behavior. The major implication, which is the foundation of reliability theory, is that failure probabilities can be computed statistically. For instance, during the steady state, the failure rate (i.e., the number of failures occuring in a given time period) does not increase or decrease. Instead, the failure rate is constant across all incremental "slices" of time during the steady state. Failures are also random during the steady state. That is, they are not due to any known cause, such as design defects (which should have been weeded out during de-bugging) or wearout. To the statistician, these characteristics indicate that the failure rate conforms to the statistical exponential distribution. By applying the proper mathematical formula for the exponential distribution, the success probability, that is, the probability of no failure can be computed.

This formula, which involves the simplest of any statistical distribution, is:

$$R = e^{-\lambda t}$$

where R is the numerical reliability, or in other words, the probability that the equipment will not fail. The failure rate is λ , e is the Napierian constant (2.718...), and t is the time period of interest.

As an example, assume that we had collected failure data on a certain type of equipment, and thus knew that it failed, on average, three times every 10,000 hours. Its failure rate (λ) would be 3/10,000, or, 3×10^{-4}. Assume also that we wish to know the probability that the equipment will not fail (i.e., the reliability) in a 1,000 hour period. Then,

$$R = e^{-(3 \times 10^{-4})(1000)} = 0.74 \text{ or } 74\%$$

Therefore, there is a 74 percent chance that the equipment will not fail during the 1,000 hour period. Conversely, there is a 26 percent chance that it will fail. (That is, there is a 100 percent chance that it will either fail or not fail, and 100 percent minus 74 percent is 26 percent.)

There are, of course, other statistical distributions than the exponential distribution. Failure data, including failure rates, have been collected and analyzed for electronic equipment for over 20 years now, and this has resulted in general agreement that the exponential distribution "fits" the steady state failure characteristics of electronic equipment. There are some indications that the failure characteristics of mechanical equipment follow some other distribution. But for simplicity and lack of an extensive statistical data base on mechanical equipment failures, the exponential distribution is usually used.

B. THE PROBABILISTIC NATURE OF RELIABILITY PREDICTIONS

The above discussion indicates that reliability predictions are probabilistic. To properly interpret reliability predictions, it is mandatory that their probabilistic nature be kept firmly in mind. For instance, a predicted reliability of 75 percent does not necessarily mean that, for a relatively small number of trials or tests, 75 percent of the time the equipment will not fail. This can be seen by considering that in a coin toss, there is a 50 percent chance of heads and 50 percent chance of tails. This does not mean that 10 tosses will yield exactly 5 heads and 5 tails. Over a large number of trials, however--say 1,000 or 10,000--about a 50-50 ratio should be observed. Similarly, over a large number of trials or tests of identical equipment during the time period of interest, the ratio of the number that fail to the number that do not fail should conform approximately to the ratio of the success-failure probabilities.

Predicted reliabilities for equipment can range from less than 1 percent to greater than 99 percent, depending on the equipment's failure rate and the time period of interest. Conversely, the probability of failure can range from over 99 percent to less than 1 percent. In interpreting the "likelihoods" associated with such percentages, it is useful to recall that a 50 percent probability indicates that the predicted event is equally likely or unlikely. That is, it is likely to occur about half the time, and unlikely to occur the other half of the time. From the 50 percent point upward, the predicted event becomes more and more likely; from the 50 percent point downward, the predicted event becomes more and more unlikely.

C. FAILURE RATES

Reliability predictions can obviously be no more accurate than the failure rates used in computing them. The most realistic equipment failure rate is one obtained from field data on a statistically valid sample of like equipments used in the same environment. Except for some military equipment, such a failure rate is seldom available because it requires failure data collected on many similar equipments over thousands of hours of operating time. Equipment failure rates generally considered the next most realistic, and the ones usually used in practice, are equipment failure rates computed from the failure rates of the piece parts (i.e., transistors, relays, motors, gears, etc.) that make up the equipment. There are several standard compendiums of piece part failure rates covering a statistically valid sample. MIL-Handbook 217--the "bible" for electronic piece part failure rates--reflects data on millions of electronic piece parts collected over billions of operating hours.

For an equipment that will fail if any one of its piece parts fail, the equipment failure rate is the sum of the piece part failure rates. Most "lower level" equipment does fail in this manner; for instance, a circuit will fail if one of its transistors fails. At "higher levels," some part failures may not cause equipment failures (for instance, the failure might effect only that portion of the equipment provided for trouble-shooting). The reliability analyst must take this into consideration. This is usually done by dividing the equipment up into its lower level components, and then treating each component according to how its failures effect the equipment.

As an example, consider a very simple piece of equipment that is made up of three identical circuits. Assume that it has been determined that failure of any circuit would cause failure of the equipment, and that failure of any piece part would cause the circuit to fail. Also assume that each circuit contains two transistors and a relay and that their failure rates are as shown.

PART	QUANTITY	FAILURE RATE PER PIECE PART
Transistor	2	0.18 failures per million hours
Relay	1	2.60 failures per million hours

The failure rate for each of the three circuits would be:

$$\underset{\text{(transistor)}}{(0.18 \times 10^{-6})} + \underset{\text{(transistor)}}{(0.18 \times 10^{-6})} + \underset{\text{(relay)}}{(2.60 \times 10^{-6})} = 2.96 \times 10^{-6}$$

The failure rate for the equipment would be the sum of the failure rates for the three circuits, or,
$3(2.96 \times 10^{-6}) = 8.88$ failures per million hours.

One of the most well known measures of reliability is MTBF (Mean Time Between Failures). MTBF is the reciprocal of the failure rate (or vice-versa). So in this example the MTBF would be $1/(8.88 \times 10^{-6})$, or, 112,613 hours.

D. RELIABILITY IMPLICATIONS OF TIME

As discussed in Section II.A, reliability predictions based on the exponential distribution are computed for some time period of interest. It is obvious that if the time period is short, the reliability will be high (or, the probability of failure will be low). This is because the shorter the period, the less opportunity for random failures to occur. Conversely, the longer the period the more opportunity for random failures, and the predicted reliabiity will be lower.

To illustrate, consider an equipment that has a failure rate of 50 failures per million hours. If we assume it operates 40 hours per week, the following reliabilities can be computed:

Reliability for 1 Week:

$$R = e^{-(50 \times 10^{-6})(40 \text{ hours})} = 99.8\%$$

Reliability for 1 Year:

$$R = e^{-(50 \times 10^{-6})(40 \text{ hours} \times 52 \text{ weeks})} = 90.1\%$$

Reliability for 3 Years:

$$R = e^{-(50 \times 10^{-6})(40 \text{ hours} \times 52 \text{ weeks} \times 3 \text{ years})} = 73.2\%$$

The failure rate used in this example (i.e., 50×10^{-6}) is in the ballpark range for many types of electronic "black boxes." The predictions indicate that it has less than a 1 percent chance of failing over a period of a week, or, that failure is extremely unlikely. Over a period of a year, with a failure probability of about 10 percent, failure is unlikely. After the equipment has been in operation for three years, however, it has about a 27 percent chance of failure, implying that over the 3-year period, it has somewhere between a one-out-of-four to one-out-of-three chance of failing.

E. RELIABILITY IMPLICATIONS OF THE NUMBER OF PARTS

It is common sense that the more parts there are in an equipment, the greater the chance that one of them will fail. This can also be seen by considering that the failure rate of an equipment is the sum of the failure rates of its essential piece parts.

Integrated circuits typically have failure rates ranging from 0.05 to 0.1 failures per million hours. This means that for a single integrated circuit to have even a 10 percent to 30 percent chance of failing, it would have to operate continuously for over 2,000 years. Most equipments, however, have at least 20 integrated circuits, and a subsystem consisting of 10 or so equipments can have more than 500 integrated circuits. With this amount of circuitry, failure is likely at some point over a 1-year period.

F. REDUNDANCY AND RELIABILITY MODELLING

In the discussions above, we have been dealing with equipment that would fail if any of its piece parts failed. There are several situations where this would not be the case. As indi-

cated above, for instance, the equipment would not necessarily fail if one of its parts provided only for troubleshooting failed. Another case would involve equipment where redundancy is utilized.

Assume, for instance, that an equipment contains a "black box A," and that for the equipment to remain operable, black box A must remain operable. Now, if two identical "black boxes A" were provided, the equipment would remain operable if either one of the redundant "black boxes A" remained operable.

In order to compute the probability that a redundant configuration is operable, the probabilities that the individual redundant items are operable must be considered. This is done according to the rules of Boolean algebra.

In our example involving two "black boxes A," call them A_1 and A_2, a truth table can be developed. In the table, an entry of 0 indicates the hardware has failed (is non-operable), and an entry of 1 indicates that it is operable. For A_1 and A_2, there will be 4 possible states--both operable, A_1 operable and A_2 non-operable, etc. For each of these possible states, the equipment will be operable (an entry of 1) if A_1 or A_2 is operable. The truth table depicting these states is as follows:

A_1	A_2	Equipment	
1	1	1	State 1
1	0	1	State 2
0	1	1	State 3
0	0	0	State 4

The probability that the equipment is operable, that is, its reliability R , can be obtained by properly combining the probabilities that A_1/A_2 are operable (R_{A_1}, R_{A_2}). In Boolean terms, where "+" indicates the logical "or", "·" the logical "and", and the bar the logical "not", the expression for our example is:

$$R_E = \underbrace{(R_{A_1} \cdot R_{A_2})}_{\text{State 1}} + \underbrace{(R_{A_1} \cdot \overline{R}_{A_2})}_{\text{State 2}} + \underbrace{(\overline{R}_{A_1} \cdot R_{A_2})}_{\text{State 3}}$$

In the above expression, the "$\overline{R}$'s" indicate that a particular black box is not operable. This is equivalent to one minus the probability that it is operable (since the probability that it is operable plus the probability that it is not operable equals 100 percent). Thus,

$$\overline{R}_{A_1} = 1 - R_{A_1}$$

$$\text{and } \overline{R}_{A_2} = 1 - R_{A_2}$$

Substituting these in the above expression yields:

$$R_E = (R_{A_1} \cdot R_{A_2}) + (R_{A_1}(1 - R_{A_2}) + (1 - R_{A_1})R_{A_2})$$

Since we have defined the two black boxes as identical, their reliabilities will also be identical. In other words,

$$R_{A_1} = R_{A_2}.$$

By referring to these simply as R_A, substituting this into the Boolean expression yields:

$$R_E = R_A^2 + 2(R_A(1-R_A))$$

Further ordinary algebraic simplification yields:

$$R_E = 2R_A - R_A^2$$

It might be wondered why it would not be correct, and far simpler, to express the probability that the equipment was operable as simply the probability that either of its black boxes were operable, or,

$$R_E = R_{A_1} + R_{A_2} = 2R_A$$

The reason is that this will not cover all the probability, whereas the state table approach does. That is, if the probabilities for all 4 states in the above table were summed, they would yield 100 percent. In other words, there is 100 percent probability that the equipment will be one of the four states identified.

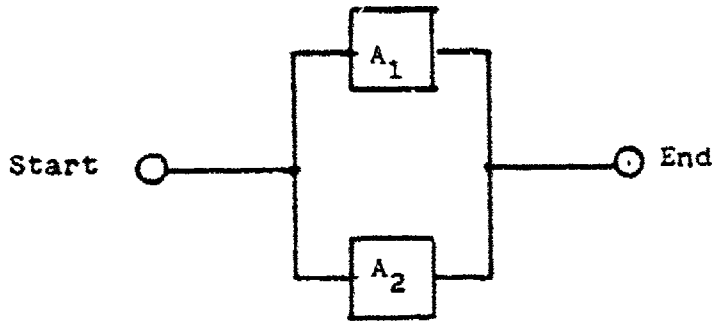
To obtain a numerical indication for this, assume that the black box reliability is 80 percent. According to the expression developed from the state table,

$$R_E = 2(.80) - (.80)^2 = 0.96, \text{ or, } 96\%$$

If we had used the expression $R_E = 2R_A$, we would have computed an R_E of 1.6, or 160 percent, which is a meaningless probability. That is, the probability of some occurrence can never be greater than 100 percent.

This example of using a truth table and combining probabilities according to Boolean logic is known as reliability modelling. Theoretically, the reliability of any system can be modelled in this manner. In practice, truth tables can rapidly become too lengthy to handle (e.g., truth tables covering three "black boxes" would contain 8 states, those for four "black boxes" 16 states, etc.). For this reason, shorthand approaches have been developed. The one most widely utilized is the reliability block diagram approach.

In the block diagram approach to reliability modelling, the success paths are depicted. In the example of the redundancy above, the block diagram would be:

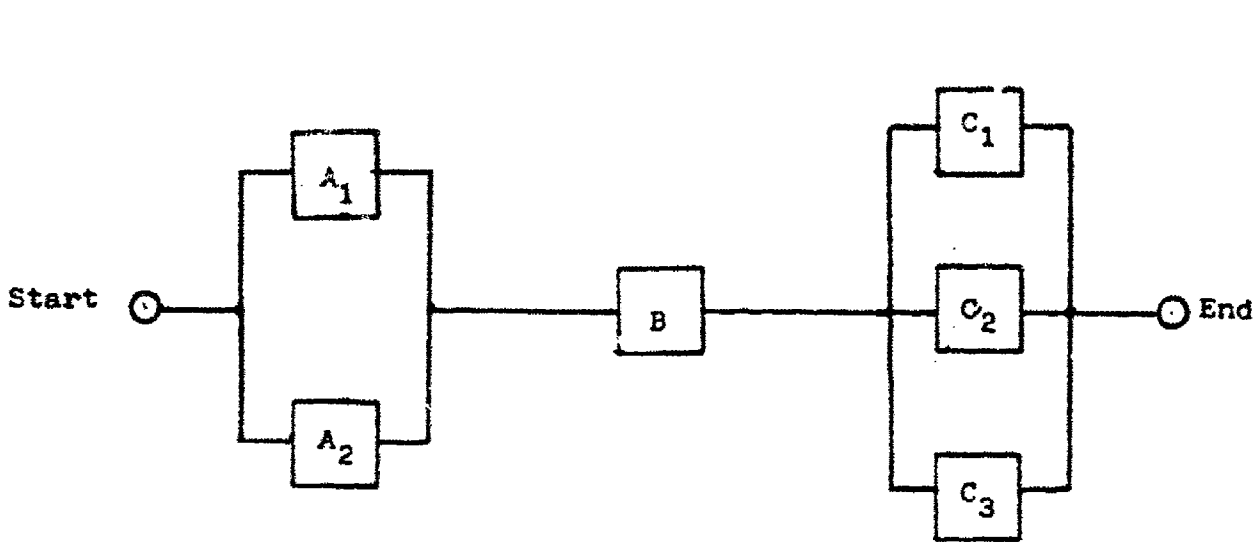


This indicates that the success path from start to end can be either via A_1 or A_2. When such a success path appears on a block diagram, the analyst knows to compute its numerical reliability from the expression developed from the truth table above, namely, $2R_A - R_A^2$. This equation, as well as those for many other block diagram configurations, are available in all standard reliability textbooks and handbooks, including MIL-Handbook 217.

G. RELIABILITY BLOCK DIAGRAMS

As can be seen from the above discussion, in order to facilitate the computation of the reliability of an equipment, its reliability block diagram should first be developed. In other words the success paths should be depicted. This, in turn, requires that the "success" of the equipment be defined in terms of the "success-failure" of each of the "black-boxes."

As an example of the process, assume we have an equipment composed of two "Black Boxes A" in the redundant configuration discussed above. Assume also that there is one "Black Box B", and that it must be operable for the equipment to be operable. Further, assume there are three identical "Black Boxes C," and that the equipment will remain operable as long as any one of the three is operable. The block diagram for this equipment would be as follows:



From this diagram, the success path can be seen to be:

a) Either A_1 or A_2 operable, and

b) B operable, and

c) Either C_1, C_2 or C_3 operable.

Because of their "parallel" relationship in the block diagram, A_1 and A_2 are said to be in parallel in reliability terminology. Similarly, Box B is in series in the reliability sense. C_1, C_2, and C_3 form another parallel arrangement and are referred to as a 1 out of 3 parallel configuration.

Computing the reliability of the equipment, that is, computing the probability that it is operable, involves computing the probability that a success path exists.

For the A_1-A_2 parallel redundancy, we know either from the equation developed from the truth table above or from a handbook that the reliability (i.e., the probability of a success path) is:

$$2R_A - R_A^2$$

Since Box B is in series, the probability of a success path is simply the probability that it is operable, or in other words, its reliability, R_B.

For the 1 out of 3 C_1-C_2-C_3 parallel configuration, the probability that a success path exists can either be derived from a truth table or obtained from a handbook and is:

$$R_C^3 - 3R_C^2 + 3R_C$$

The probability that the equipment is operable, or its reliability R_E, is the probability that a success path exists from "start" to "end" in the reliability block diagram. From the individual success probabilities above, this can be seen to be:

$$R_E = (2R_A - R_A^2)(R_B)(R_C^3 - 3R_C^2 + 3R_C)$$

R can be computed by obtaining failure rates for the "black boxes" so that values can be obtained for R_A, R_B, and R_C. The overall objective of reliability modelling and block diagramming, however, does not consist solely of obtaining "numbers." Insights more valuable than numerical results can often be gained, especially with complex systems where reliability relationships would remain obscure without modelling. For instance, in the example above, it can be seen that Box B governs the reliability of the equipment. The numerical reliability of the equipment can never exceed the numerical reliability of Box B, therefore, reliability improvement efforts should focus on Box B.

H. RELIABILITY IMPLICATIONS OF PART FAILURE RATES

Over the past two decades, many thousands of man-hours have been spent analyzing electronic part failures and failure rates. Through these efforts, an extensive body of information has been acquired; the primary reference source for this information is MIL-Handbook 217.

Failures and failure rates for non-electronic parts (mechanical, pneumatic, electrical, etc.) have received considerable, though less extensive, analysis. Thus, in general, less data is available on failure rates for non-electronic than for electronic parts. Also, while little numerical data is available on failure rate contributing factors for non-electronic parts, a significant amount exists for electronic parts. Though this numerical data on failure rate contributing factors for non-electronic parts is scarce, there is general agreement that the same basic factors contribute to failures in both electronic and non-electronic parts. For electronic parts, these factors--together with their numerical values for various conditions--are given in MIL-Handbook 217.

Probably the most important implication of these failure rate contributing factors is that "improving" the factors will improve the failure rate. This can be seen by considering the method of determining a part failure rate from MIL-Handbook 217.

In this handbook, part failure rates are given in the form of a base failure rate multiplied by modifying, or K-factors. That is,

$$\lambda_p = \lambda_b \cdot \pi_{k_1} \cdot \pi_{k_2} \cdot \cdots$$

where λ_p is the failure rate for the specific part under consideration (for instance, a PNP power transistor). λb is the base failure rate for the generic category of parts (for instance, PNP transistors). To obtain the part failure rate (λp), the generic base failure rate (λb) is multiplied by the appropriate K-factors. These K-factors reflect failure rate contributing factors that impact the base failure rate multiplicatively. That is, they increase or decrease the base failure by some multiple. The base failure rate, λb, also reflects failure rate contributing factors, but rather than being direct multiples, these contributing factors impact the failure rate exponentially. To illustrate, the part failure rate for a silicon PNP power transistor is developed below.

The MIL-Handbook 217 expression for transistor failure rates is:

$$\lambda_p = \lambda_b(\pi_E \pi_A \pi_Q \pi_R \pi_{S_2} \pi_C)$$

For transistors, λ_b is a function of junction temperature and the ratio of applied to rated power. Therefore, junction temperature and this power ratio are contributing factors to the failure rate, and as indicated above, the relationship is exponential. The lower the value of these factors, the lower, or "better", the failure rate. A transistor that has been de-rated so that the ratio of applied power to rated power is 30 percent, and that is operating at a junction temperature of 70° C, has a base failure rate of 0.0023×10^{-6}. If the power stress ratio (i.e., the ratio of applied to rated power) is 60 percent, and the junction temperature is 80° C, the base failure rate for the same device is 0.0077×10^{-6}, or over three times the base failure rate for benign conditions.

In the failure rate equation above, π_E is a K-factor that accounts for the part's operating environment. For a "ground benign" environment, i.e., the typical environment within a building, π_E has a value of 1.0. For the "naval sheltered" environment, i.e., on shipboard but not on on-deck or exposed to the elements, π_E has a value of 9.8. For the "naval unsheltered" environment, π_E is 21.0.

The π_A factor in the failure rate equation is an application factor, and accounts for the way the part is used. If the part is used in a "switching" application (as in logic circuitry), π_A has a value of 0.7. If the part is used in a "linear" application (as in analog or power circuitry), π_A is 1.5.

The next factor, π_Q --the quality factor--represents a failure rate contributing factor that offers significant possibilities for failure rate improvement. It is a function of the level of quality control applied by the part manufacturer. For transistors, π_Q for the lowest quality level is 12.0. This level covers plastic encapsulated, commercial parts which are subjected to the fewest qualtity control measures, and are sold

essentially as they come off the assembly line. For the next lowest quality level, π_Q is 6.0. Quality control measures at this level include use of better materials (non-plastic), and some checking and screening after the parts come off the line. For the highest quality level, which includes stringent materials and manufacturing controls, screening and burn-in, π_Q is 0.12. Thus the transistor failure rate can vary from 0.12 to 12, or, a factor of 100, depending on the part's quality level.

The π_R factor in the failure rate equation above accounts for the power rating of the transistor. It ranges from a low value of 1.0 for transistors rated at 1 watt or less, to a high of 5.0 at ratings of 50 watts and above.

π_{S_2} is the voltage stress factor, and is the ratio of applied to rated voltage. For ratios of 50 percent (i.e, the applied voltage is half the rated voltage), π_{S_2} has a value of 0.65. For a ratio of 100 percent, π_{S_2} is 3.0, which implies over a three-fold increase in the part failure rate.

π_C is the complexity factor, and relects how the transistor is interconnected within its package. For a single transistor in a TO-5 can, π_C is 1.0; for a dual transistor in a Darlington configuration, π_C is 0.8.

The table below depicts how the part failure rate can vary for the same transistor for the same application. "Low" and "high" values were used only for those factors within the designer's control. For instance, the value of π_E is for the naval sheltered environment in both cases because the designer generally cannot change the operating environment of the equipment.

As can be seen from the table, the part failure rate for the transistor can be improved over 150-fold through factors within the designer's control. Similar failure rate improvements are possible with other types of parts. For electronic parts, MIL-Handbook 217 can be consulted to identify the applicable factors. This handbook is periodically revised, and the current version is MIL-Handbook 217D. For non-electronic parts, the rationale is the same even though specific data are scarce. That is, failure rate improvements can be gained through de-rating, improved quality control, improved operating environment, etc.

Table II-1
Part Failure Rate

Failure Rate Parameter	"High" Value	"Low Value"
λ_b (base failure rate)	0.0077×10^{-6} for power stress ratio of 60% and junction temperature of 80° C.	0.0023×10^{-6} for power stress ratio of 30% and junction temperature of 70° C.
π_E (environmental factor)	9.8 (naval sheltered)	9.8 (naval sheltered)
π_A (application factor)	1.5 (linear application)	1.5 (linear application)
π_Q (quality factor)	12.0 (plastic, commercial)	1.2 (JAN level)
π_R (power rating factor)	2.0 (for 5 to 20 watt power rating)	2.0 (for 5 to 20 watt power rating)
π_{S_2} (voltage stress factor)	3.0 (for ratio of 100%)	0.65 (for ratio of 50%)
π_C (complexity factor)	1.0 (single transistor in can)	1.0 (single transistor in can)
λ_p (part failure rate)	8.15×10^{-6}	0.053×10^{-6}

I. FAILURE MODES AND EFFECTS ANALYSIS

One of the most important "tools of the trade" of the reliability engineer is the Failure Modes and Effects Analysis--FMEA, or the Failure Modes, Effects and Criticality Analysis--FMECA. Through this analytical approach, possible failure modes are identified, then their effects are determined. Usually, the criticality of the failure effects is also determined.

In performing an FMEA or FMECA, the level to which the analysis will be conducted is first established. Depending on the circumstances, this can be to the part level (e.g., transistor, NAND gate, solenoid valve, limit switch, etc.), to the

"circuit" level (e.g., flip-flop, amplifier, servo-loop, etc.), or in complex systems, to the "black box" level (e.g., communications receiver, computer memory module, hydraulics assembly, etc.). Obviously, the "lower" the level considered--e.g., the part level or "circuit" level--the more detailed the information produced concerning how the equipment will behave under potential failure conditions.

The various hardware "elements" are then considered individually, For each element, possible failure modes are identified. For instance, for diodes possible failure modes include fail-open and fail-short; for NAND gates, fail-high and fail-low, etc. The failure effect is then determined for each failure mode. This is usually done at two levels, the subsystem or "component" level, and the system level.

The subsystem failure effect if a particular diode failed open, for instance, could be that a certain signal would never "go active," in turn, preventing some particular device from ever being actuated. The system failure effect, then, would be the effect on system operation if this device could not be actuated--for instance, "astern valve could not be opened, causing loss of ability to go astern."

Criticality can then be evaluated, and of particular significance, the specific parts or "elements" which can cause critical failure effects can be identified. Through this identification, critical failure effects can be eliminated through alternate design approaches , or their likelihood can be reduced through reliability improvement, for instance, by improving the failure rates of the parts.

III. GENERAL DISCUSSION OF CONTROL SYSTEMS

Modern automated propulsion control systems are designed to replace the watchstander and such human senses as sight, sound, touch, smell, etc.. Besides being designed to replace the human element, the systems --- if designed and functioning properly ---will perform more efficiently than the human watchstander. But as with any system, there is no such thing as a perfectly designed system which always functions as intended. Therefore, the human interface cannot be entirely eliminated. With proper design and due consideration for reliability and maintainability, the human interface can be minimized but never eliminated.

In the subsections which follow, the general aspects and design functions of automated propulsion control systems are described. The functions discussed can be seen to be those that either replace a function once performed manually, or provide some type of interface function between the equipment being controlled and the watchstander.

A. STEAM TURBINE CONTROL SYSTEMS

Automated propulsion controls for steam vessels can be broken into three major categories: boiler control, turbine control, and auxiliary control. Within each category, a number of functions are performed.

A.(1) Boiler Control

Boiler controls generally include safety shutoff provisions, equipment for ignition sequencing and proving, control loops for combustion control parameters, programming for start-up and shutdown, and sensing provisions for such abnormal conditions as flame failure. The control system senses and makes the boiler respond to changes in steam demand and it trips the boiler when an unsafe condition arises.

The following are the subsystems usually found within the boiler control system. The function of these subsystems together with how the subsystems interact with each other, is described in general terms.

A.(1)(a) Condensate Control System

The condensate control system provides the low pressure link to close the steam and feedwater cycle. It also insures a

reserve water capacity, usually in the deaerating feed tank, to cover water flow transients.

A.(1)(b) Combustion Control

When steam flow from the boiler increases, there will be a slight drop in superheater outlet pressure because of the increased steam flow. A temporary rise in the drum level will occur because the slight drop in pressure of the saturated liquid causes bubbles of increased evaporation. The heat stored in the boiler water and metal parts, and the water stored in the boiler drum, supply the first portion of the transient increase in steam flow without any initial corrective action by the control system.

Signals representing the increased steam flow and the decreased superheater outlet pressure are summed to give a fuel/air master demand signal. This master demand signal goes to the fuel/air control system to increase the firing rate.

The fuel/air system monitors actual air flow to the burners by measuring pressure drops across the burner throat. It monitors fuel flow by sensing the position of the fuel oil control valve. On receiving a signal to increase firing, the controllers first send a signal to the forced draft fan damper actuators to increase air flow. After the air flow has been increased and sensed at the burners, the fuel valve is moved to the new flow setting required by the increased steam flow.

The fuel/air system is then balanced by the controls at the firing rate required to restore the set value of superheater outlet pressure and the set value of the fuel/air ratio.

A.(1)(c) Drum Level Control

The drum level controller ignores the small rise in drum level because it has received an increased steam flow signal as well. A little later, however, the drum level will start to drop, and the decrease in drum level signal combined with the increase in steam flow signal will cause the drum level controller to reposition the feed water control valve to give more water flow to the boiler drum.

Fuel, air, and water are now reset to the newly required values to accommodate the increase of steam flow.

A.(1)(d) Fuel Oil Pressure Control

To permit using fuel oil valve position as a flow indication, the fuel oil control valve differential pressure is monitored and held constant by adjustment of a fuel header bypass

valve. Fuel oil viscosity is held essentially constant by controlling fuel oil temperature through regulation of the steam supply to the fuel oil heaters.

A.(1)(e) Superheated Steam Temperature

The superheater outlet temperature controller holds the set temperature by adjusting the amount of desuperheated steam bled into the system from the control desuperheater in the water drum.

A.(1)(f) Feedwater Pressure Control

When a variable speed feed pump is used, two control methods are in general use today. In one method, a controller regulates pump discharge pressure by adjusting pump speed. The feed water flow is measured by the differential pressure across an orifice in the feed line to the boiler. In the second method, the speed of the pump is controlled to maintain a constant pressure drop across the feed water control valve. The feed water control valve position may then be used as a feed flow measure.

In cases where a constant speed feed pump is used, the usual arrangement is to measure feed flow with an orifice, and to control flow with a feed control valve.

A.(1)(g) Burner Management

The burner management logic controls the automatic boiler purge and light-off sequence. Also, the logic usually controls the fuel oil recirculation function and the boiler shutdown logic. All control systems automatically shut down the boiler when the following occurs:

a) Loss of flame.

b) Drum level low low.

Some systems also provide for other trip logic which will shut down the boiler. Some of these are:

a) Air flow low.

b) Fuel oil pressure low.

c) All burner valves closed.

d) Unsuccessful burner shutdown.

A.(2) Turbine Controls

Automated turbine control systems control the flow of steam for ahead or astern propulsion. The most commonly used system incorporates two propulsion control loops. The primary loop positions the steam valves as a function of the throttle lever setting, which in turn is approximately proportional to propeller RPM. The secondary or speed feedback loop, which is used during maneuvering, positions the steam valves to maintain shaft revolution at a constant value as established by the throttle lever setting. In addition to propulsion control, the turbine control usually contains the following auxiliary control features:

a) Automatic rollover of shaft when throttle is in the stop position,

b) Automatic RPM reduction when an abnormal condition occurs, and

c) Turbine trip when extreme conditions occur.

A.(3) Auxiliary Control

The auxiliary controls start standby pumps, regulate the voltage and frequency of electrical power, control pressure and temperature of lubricating oil, and serve other functions usually associated with direct acting, on/off or direct proportional controls.

B. DIESEL VESSEL CONTROL SYSTEMS

Diesel propulsion system controls perform, as a minimum, two overall functions, namely 1) automatic or semi-automatic engine start-up and shutdown, and 2) automatic engine speed control based on thrust requirements. Other overall functions depend on the specific system and may include clutch control and propeller pitch control.

Engine start-up is primarily a semi-automatic function in that it is manually initiated (for instance, by depressing a push-button switch). Subsequent start-up control actions are fully automated. These involve first checking automatically to ascertain that engine start-up is permissible. To accomplish this, sensor signals are "checked" by the controls to determine if all start-up permissives are met. These permissives include adequate fuel oil and lube oil pressure and jacket water temperature, barring gear disengaged, etc..

If all start-up permissives are met, the automatic sequence proceeds by signalling the engine to initiate the start-up pro-

cedure. The exact procedure will vary somewhat depending on the specific engine but generally involves purging the crankcase, rolling the engine on starting-air, admitting the fuel oil supply, etc.. In most present systems, these latter procedures are under the control of hardware provided on the engine itself (that is, remote from the engine control console), and are supplied by the engine manufacturer.

Engine shutdown is both automatic and semi-automatic. Automatic shutdowns are initiated when a condition exists that could cause engine damage (for instance, low lube oil pressure). Sensor signals are continuously "checked" automatically to determine if such a condition exists. Semi-automatic shutdowns are manually initiated by depressing a shutdown switch on the console. Subsequent procedures are the same for either type of shutdown, and are controlled automatically. These generally involve sending a shutdown signal to control equipment provided on the engine which, in turn, shuts down the fuel oil supply.

Automatic engine speed control is usually implemented through use of a classical, feedback control loop. This loop consists of the throttle lever, some type of device to simulate the engine's speed vs. power curve, a device to provide actual engine speed, and an error signal generator. Signals from the throttle lever are used in the loop to determine the desired engine operating point on the speed-power curve. This desired engine operating point is compared with the actual operating speed by the error signal generator. If the desired and actual points are identical, no error signal is generated. If they are not identical, an error signal is generated which indicates whether actual speed is too slow or too fast. This error signal is transmitted to the engine where it is used to increase or decrease engine speed.

Other functions performed by the automatic controls can include clutch control and propeller pitch control. Clutch control consists of activating or de-activating some type of clutch actuator. Generation of the activate signal is based on checking for the presence of all clutch engage permissives. These include proper engine speed and proper synchronization of engine speeds when the vessel has more than one engine. The activate process is usually initiated semi-automatically via depression of a pushbutton switch. The de-activate process can be initiated via a pushbutton switch, by some condition that would cause machinery damage if the clutch remained engaged, or by engine shutdown.

Automatic propeller pitch control again usually utilizes a classical, feedback control loop. This loop consists of the throttle lever, some type of device for correlating engine speed and load with the propeller pitch angle, a device to provide actual propeller pitch, and an error signal generator.

Signals from the throttle lever are used in the loop both to indicate pitch direction (i.e., ahead or astern), and to indicate the desired vessel speed. This desired speed and direction signal is correlated with engine speed and load to determine the actual propeller pitch required. The error signal generator then compares this required pitch with actual pitch. If the required and actual points are identical, no error signal is generated. If they are not identical, the error signal indicates the direction and magnitude of the error. This error signal is sent to the propeller unit to control pitch actuation.

IV. LITERATURE REVIEW

Task I of the DOVAP study consisted of a search and review of the open literature. The effort focussed on marine automation systems and their reliability and maintainability characteristics. Over 250 documents were reviewed, from which 115 were deemed applicable to the study. Summaries of the pertinent contents of these applicable documents were prepared. In addition, a document log was prepared, and a cross-reference matrix for accessing the documents was developed.

In the following subsections, the approach to, and the findings of, this literature search are described. The individual document summaries, the document log, and the cross-reference matrix are provided in Appendix A.

A. LITERATURE SEARCH APPROACH

The literature search conducted as Task I of the DOVAP study was structured to consist of four subtasks, viz, 1) an abstract and title search, 2) document acquisition and review, 3) summarizing and cross-referencing pertinent document contents for further reference, and 4) evaluation of the pertinent documents to obtain overall findings and conclusions. Each of these four subtasks is discussed below.

A.(1) Abstract and Title Search

The major objective of this subtask was to ensure consideration of any document that might be pertinent to the reliability of large commercial vessel automation systems. Toward this end, abstracts were reviewed to the extent possible since it was felt that an abstract review, as opposed to a title search, would provide better insights into the actual contents of the document. In cases where abstracts were not available, title searches were conducted. Abstracts were generally available, however, so that search by title alone was seldom necessary.

The major abstract compilation searched was that of the Maritime Research Information Service (MRIS). These abstracts were reviewed for the period from January, 1973 to June, 1981. In addition, the MRIS Current Awareness Series for 1981 was reviewed. The MRIS abstracts cover symposium papers, contract reports, and such publications as the Naval Engineer's Journal and the Journals of the Society of Naval Architects and Marine Engineers. Hence, the MRIS abstracts provide quite comprehensive coverage.

National Technical Information Service (NTIS) abstracts were also searched. There is considerable overlap between MRIS and NTIS, but NTIS provides more complete coverage of U.S. Navy contract reports.

A cursory review of "Ship Abstracts," a joint Norwegian-Swedish-Dutch-Finnish information service, was conducted. A majority of the documents abstracted, however, were not in English, and those in English were found to be also covered in MRIS.

In addition to the abstract searches noted above, library searches were conducted to ensure thorough coverage of the literature. This part of the effort focussed on recent documents that might be too recent to be covered by MRIS and NTIS. Also, cumulative indexes of maritime publications were checked by title to ascertain that pertinent documents were not overlooked.

A.(2) Document Acquisition and Review

From the abstract and title search, over 250 documents were identified as possibly pertinent, and were ordered. Of these, only six could not be obtained. As could be expected, many of the documents were found not to be pertinent once they were reviewed. Also, as more documents were reviewed, considerable repetition between documents was noted. Nevertheless, 115 documents ranging from good to excellent in terms of their applicability to the DOVAP study were reviewed.

Since both reliability and automation systems encompass a wide range of factors, applicable documents also cover a broad spectrum of topics. For instance, maintainability is of interest because proper preventative maintenance can enhance reliability, and improper maintenance can result in equipment malfunction. The state of the art is of interest because it indicates the "maturity" of the equipment and hence whether early design and development problems can be expected. Environmental factors are of interest because failures can occur due to overstress if the equipment is subjected to environmental parameter levels that exceed design levels.

The documents identified as applicable to the DOVAP study can be divided into nine broad categories of topics. These are as follows:

a) R&M Quantitative Data: Failure rates, failure frequencies, repair rates, equipment availability, etc.

b) R&M Qualitative Data: Failure mode descriptions, operating experience/problems, preventative maintenance procedures, quality assurance provisions, etc.

c) Maritime R&M Status Information: Extent and nature of R&M practiced in the maritime community.

d) Automation Configuration Information: Types of hardware items and systems, and what functions they must perform.

e) Automation State of the Art: Degree of maturity, or point on the "learning curve" the equipment has achieved.

f) Spare Parts Assessments: Availability of spare parts for repair, on-board spare parts provisionning practices, spare parts problems, etc.

g) Regulations/Requirements: Mandatory and non-mandatory requirements for automation system design, analysis, construction test, etc.

h) Environmental Information: Natural and man-made environmental factors which can impact equipment operation.

i) Other: Emerging trends such as condition monitoring; training/skills; system documentation/maintenance manuals; predictions/projections of maritime trends/potential problems; etc.

The contents of some of the applicable documents fell into more than one of the above broad categories. Other documents concentrated on topics in a single category. The portions of the document pertinent to the DOVAP study ranged from a few paragraphs or a few sentences to the entire document.

A.(3) Summarization and Cross-Referencing

Due to the large number of documents received and reviewed, a method of coding them for easy access was required. To accomplish this, a four-step procedure was employed. This consisted of (1) a document logging scheme, (2) preparation of summary sheets, (3) assignment of category codes for cross-reference and (4) preparation of narrative summaries of the pertinent information.

The document log consists of a straightforward index card file and log sheet system. All applicable documents are referenced and accessible by their respective log numbers. The log sheets are provided in Appendix A.

Forms were developed for summarizing the applicable document information. The intent of these forms was to provide

accessiblity to pertinent information within the document. Since many of the documents were on microfiche, locating pertinent information within the document could have proved troublesome without this scheme. These summary forms were completed as the documents were reviewed.

The summary sheets noted above were not intended to provide accessiblity across all documents. To accomplish this, a subject categorization/accessing code system was implemented. This consists of an indentured breakdown of subject categories together with a code number for each category. Documents were assigned as many code numbers as were applicable, and the code numbers were entered onto the document's card in the log file. A cross-reference matrix was also prepared that indicates the documents, by log numbers, containing information in the various subject categories. This cross-reference matrix is provided in Appendix A.

Narrative summaries of each applicable document were also prepared. These summaries are again provided in Appendix A.

In preparing these narrative summaries, no attempt was made to "judgmentally" evaluate the documents. Instead, every attempt was made to objectively summarize the portions of the document that could be applicable to the DOVAP study, or possibly to any other study involving maritime reliability and maintainability and/or marine automation systems.

B. LITERATURE SEARCH FINDINGS AND CONCLUSIONS

This section describes overall and specific findings and conclusions of the Task I Literature Search. In addition, some observations resulting from the literature search are noted. These observations are as follows:

a) It appears that very little formal, systematic reliability engineering is applied during commercial vessel design activities. The reliability engineering that is applied seems to consist primarily of qualitative judgments as to how well the equipment can be expected to perform.

b) Increasing maritime accident rates provide a strong argument for the need for more detailed and in-depth R&M considerations.

c) The terms "reliability" and "maintainability" are often used loosely in the literature, and appear to mean different things to different people. Many use the terms to convey some intuitive measure of equipment "worth." The terms, and reliability especially, were often not used in the sense of

their established, theoretical framework.

d) A general awareness of current reliability problems (e.g., areas known to be troublesome) was evidenced in the literature, and good qualitative evaluations of them were provided.

A number of overall and specific findings and conclusions of the literature search were developed. These are presented below under the nine category headings cited for the applicable documents in section A above.

B.(1) R&M Quantitative Data

About forty documents provide marine R&M quantitative data of various types. The more extensive of these data sources were developed for the Navy. Log #508 is a particularly comprehensive tabulation of R&M data (MTBF's, MTTR's, etc.) developed for Navy mechanical equipment. The non-Navy documents provide a "scattering" of MTBF's, availabilities, and failure frequencies. While these are not comprehensive enough to use alone, they were used during subsequent phases of the study in developing "K" factors for adjusting failure rates from other sources. Such adjustment is necessary, for instance, to convert Navy failure rates which reflect MIL-SPEC quality levels to values reflecting commercial quality levels.

Considerably more quantitative reliability data was found than maintainability data, with Navy documents providing almost all of the maintainability data. Since Navy maintenance policies and approaches differ considerably from commercial practices, it appears that even with adjustment, Navy maintability data would have to be used judiciously for commercial applications.

The summaries of some of the more pertinent papers dealing with quantitative data are presented below. As indicated above, most of this data was used later in the study in developing K-factors for adjusting failure rates for non-commercial equipment to those applicable to commercial equipment or to determine the correlation between the historical data and the predicted values.

B.(1)(a) Log #106

This document investigated two aspects of equipment behavior, i.e., reliability and degradation. This data was collected on Navy shipboard machinery. Routine maintenance data on the shipboard machinery were analyzed to identify failure and degradation trends. The maintenance actions considered were those occurring since the last ship overhaul. The paper concluded that the reliability of some ship's equipments tended to decrease with age, and that the number of maintenance actions

increased. As an example, the paper shows that for main boilers, the mean operating hours to first failure is 1,050. The mean operating hours to the second failure of boilers was 875 hours. Because some equipments exhibited an increasing maintenance rate over their operational lives, the commercial operator must anticipate this increased maintenance demand.

B.(1)(b) Log #026

This document reports on a study comparing the reliability of single boiler and multiple boiler vessels. Reliability is based on casualties, where casualty is defined as: (a) actual physical damage of property in excess of $1,500; (b) material damage affecting the seaworthiness or efficiency of the vessel; (c) stranding or grounding; (d) loss of life; (e) injury causing any person to remain incapacitated for a period in excess of 72 hours. This data was obtained from commercial vessel information related to the above mentioned casualties supplied to the Coast Guard. In this data, the total of casualties for multi-boiler vessels was 3,912. The number of multi-boiler ship-years was 3,854, which yields a ratio of the number of casualties to the number of shipyears of 1.015. This is undoubtedly a conservative number because it is suspected that many minor casualties are not reported. These figures appear to include primarily major boiler damage due to explosions and major structural failures.

B.(1)(c) Log #008

This paper describes experiences with unattended engine room operation in 6 turbine tankers. More than 20 ship-years of accumulated history are represented in the data. The paper reports that casualties have occurred on some of the ships, with some of these resulting in serious damage, such as a major gear fracture and two groundings. However, the paper reports that none of these casualties were caused directly or indirectly by the automation systems. It also reports that the automation systems have not been responsible for delays in port or reduced performance.

The paper lists all alarms for the six ships and classifies them as: (a) true alarms; (b) alarms resulting from maneuvers or exceptional operation; (c) false alarms. Figure IV-1 shows the average number of true alarms per month for the six ships over a six-year period. It is interesting to note that it takes approximately three years before the number of alarms stabilizes, and that after the fifth year the number slightly increases. Alarms resulting from maneuvering also show a sharp decrease after the first year and stabilize after the second year. Again, false alarms decrease after the third year and then stabilize. The nature of the alarms is given in the paper, and Table IV-1 shows the approximate distribution of alarms by causes. Breaking out the alarms by the subsystems covered in the DOVAP study yields an alarm rate of 3.5 per month, which

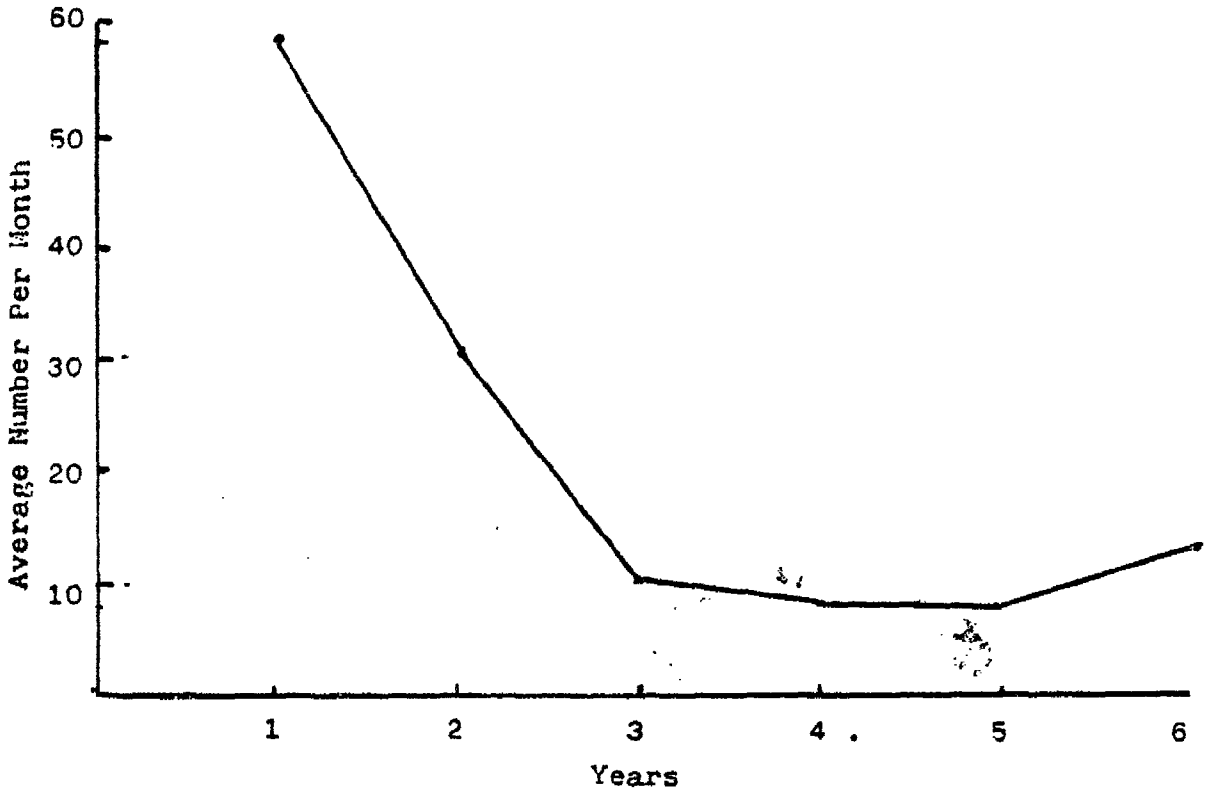


FIGURE IV-1

Number of True Alarms for Six-Year Period
(from Log #008)

Table IV-1
Average No. of Alarms per Month, 6 Ships (From Log #008)

Alarm	Parameter	No/Month: 6 Ships	Alarms Which Would be Included In Current Study
F.O. Filter	Δ P	87.2	
Evaporator	Salinity High	13.1	
Drain Tank	Level Lo	8.8	
Air Compressor	-	6.2	
Sterntube L.O. Hdr. Tank	Level Lo	5.7	
Dirty Oil Tank	Level Hi	5.35	
Desuperheated Steam	Temp Hi	4.2	
Superheated Steam	Temp Hi	4.1	*
Mn. Propul. Unit	Trip	3.8	*
Mn. Boiler F.O. Valve	Trip	2.85	*
Starting Air Comp.	-	2.5	
Water in F.O. Bunker	-	2.2	
F.D. Fans	Stop	1.7	
Main Boiler	Lo-Lo Level	1.65	*
Flame Failure	-	1.5	*
Gland Steam	Pres. Lo	1.5	
Feedwater	Pres. Lo	1.5	*
Exh. Steam Line	Pres. Hi	1.3	
Drain Tank	Level Hi	1.3	
F.O. to Burners	Pres. Lo	1.0	*
Main Circ. Pump	Fail to Start	1.0	
F.D. Fan	Oil Pres. Lo	1.0	
Exh. Steam Line	Pres. Lo	0.9	
De-oiler	Δ P Lo	0.8	
Main Boiler	Level Hi-Hi	0.75	*
Superheated Steam	Temp. Lo	0.7	*
Auxiliary Boiler	Lo-Lo Level	0.7	*
Deaerator	Level Lo	0.7	*
Oil in Observation Tank	-	0.7	
Main Boiler	Level Lo	0.65	*
T.A. Tripping Out	-	0.5	
Auxiliary Boiler	Level Hi-Hi	0.5	*
Lack Combust. Air	-	0.5	*
Blackout	-	0.5	*
Main Boiler	Level Hi	0.3	*
Oil T.A.	Pres. Lo	0.25	

Total Included in Current Study = 21.3
Average Per Ship Per Month = 3.5

the DOVAP study yields an alarm rate of 3.5 per month, which correlates with those predicted for Ships A and B (the steam turbine vessels) in the DOVAP study.

B.(1)(d) Log #097

This document reports on a study of a group of very large crude carriers (VLCC) operated by the Shell Oil Company. These ships are foreign-built and are designed for unmanned machinery operation. Between January, 1973 and June, 1977, Shell International Marine commissioned 25 of these VLCC's, a new class designated as the "L" class. The ships are turbine driven, and were built by six different shipyards. Consequently the instrumentation and controls are somewhat different, although basic specifications are the same.

In January of 1978, Shell initiated a study to evaluate the operational experiences with the instrumentation and control systems and to determine the factors that affected their reliability. From the data presented in this paper, DOVAP concluded that the "L" class vessels' instrumentation and controls are considerably more complex than those of the three systems considered during the DOVAP study. In the case of the "L" class vessels, there are 175 alarm-type surveillance systems and 85 automatic shutdown systems, with 28 of the latter being associated with the propulsion plant.

The data base for the study reported in this paper was generated from the Shell International Marine Defect Casualty Reporting System. After reviewing the data, it seems obvious to DOVAP that not all incidents are reported. The paper does state that only incidents resulting in delays or in the need for replacement parts are documented. The data covers 62 ship-years, or roughly one-half million ship hours. The total number of failure or malfunction incidents reported was 414, which amounts to 6.6 per ship-year. Again, it seems obvious from the number of malfunctions that the total number of occurrences are not being reported. However, this reported data is useful for comparative purposes. Also, it is the only data found where the relative number of failures for flame scanners, carbon dioxide systems, oxygen analyzers, and smoke density systems can be determined.

The following was extracted from the data reported in this paper and is indicative of the magnitudes of various problems related to automated control systems on the "L" class vessels.

BOILER TRIPS: Of the total 414 reported faults, 28 were boiler trips. Table IV-2 gives the causes of the 28 trips and their percentages of the total.

BURNER RELIGHT INHIBITS: There were 25 incidents which prevented relighting of the burners. The causes and percentages of these are given in Table IV-3.

TABLE IV-2

Reported Faults Resulting in Main Boiler Auto-Shutdown
(Log #097)

	Number of Incidents	Percent of Total
Force draft fan trip due to transmitter controller and broken control air lines	8	28.6
Fuel valve relay fault	6	21.4
Erroneous flame-failure trip	4	14.3
Erroneous drum level hi-hi and lo-lo trip	4	14.3
Fuel valve switch fault	2	7.1
Erroneous superheater high temperature trip	1	3.6
Combustion air flow transducer fault	1	3.6
Waterlogged atomizing steam line due to undersized drain trap	1	3.6
Drum level controller fault	1	3.6
Total	28	

TABLE IV-3

Reported Faults Inhibiting the Relighting of the Burners
(Log #097)

	Number of Incidents	Percent of Total
Timer faults	13	52
Ignitor and ignitor transformer faults	5	20
Faults on printed-circuit boards	4	16
Air register solenoid valve faults	2	8
Flame scanner faults	1	4

POTENTIAL LOSS OF PROPULSION: In addition to outright boiler trips, there were 62 incidents that could have resulted in loss of propulsion; these are depicted in Table IV-4.

TOTAL NUMBER OF INCIDENTS BY SYSTEM: Table IV-5 gives the total number of incidents by system and the percent contribution of each system. This breakdown indicates that burner management is the largest contributor to total system unreliability. The description of burner management on the L-class vessels indicates that it is a binary control system with numercus interfaces, e.g. level switches, pressure switches, flame detectors, and solenoid valves. The description of the system also indicates that the same operational philosophy is applied as on the two turbine ships investigated in the DOVAP study. However, the L-class systems appear to be somewhat more complex because of the number of alarms and trip possibilities.

COMPONENT FAILURES: Table IV-6 depicts the types of component failures that cause system failures. This data shows that the primary causes of system failure are circuit cards, followed closely by transducers.

B.(1)(e) Log #083

Log #083 reports on a reliability study of marine turbine plants based on data gathered over the one year period from April 1, 1977 through March 31, 1978. The study covers thirty-one vessels, of which 29 were tankers. The age of seven vessels was 2 years and under; the age of fifteen vessels was 2.1 to 4 years; the remaining vessels were over 5 years old. The paper breaks down the total failures experienced by component and system, and by major failure modes, and also by type of steam plant, age of ship, MO certified, ship state when failure occurred, effect of failure on ship operation, and method of failure detection.

Some of these statistics of interest have been excerpted and are presented in Table IV-7. There was a total of 31 stoppages at sea, or an average of 1 per ship for the year. It is reported that the hours for stoppages at sea was 248.6, or an average of 8.2 hours per stoppage. There were 41 occasions during the year when the vessel proceeded at reduced RPM, with a total time for reduced RPM of 854.4 hours, or an average of 20.8 hours per occasion. The failure breakdown by components shows that the major contributor to stoppage at sea was the main engine, and that the principal contributor to reduced RPM was the boiler system. Although the data did not clarify criteria for dead in the water (DIW) and reduced RPM, DOVAP suspects that temporary short-term stoppage or reduced RPM's were not included in the data because of the low number of reduced RPM occurrences.

TABLE IV-4

Reported Faults that Could Have Resulted
in the Loss of Propulsion
(Log #097)

	Number of Incidents	Percent of Total
Flame scanner fault	13	20.9
Erroneous drum level indication-- Transmitter fault	9	14.5
Erroneous superheater high temperature-- Transmitter fault	7	11.3
Erroneous fuel oil signal-- Transmitter fault	7	11.3
Burner management relay faults	5	8.1
Drum level error due to controller	5	8.1
Air register and fuel valve solenoid fault	4	6.4
Control circuit card faults	2	3.2
Feed pump timer fault	1	1.6
F.D. fan mechanical breakdown	1	1.6
F.D. fan solenoid valve fault	1	1.6
Combustion air controller fault	1	1.6
Flame scanner motor fault	1	1.6
Drum pressure-- Transmitter fault	1	1.6
Feedwater valve fault	1	1.6
Superheater spray cooler valve motor fault	1	1.6
Drum level timer fault	1	1.6
Drum level relay fault	1	1.6
Total	62	

TABLE IV-5

Total Number of Incidents by System (Log #097)
Excluding Failures Not Related To Current Study

System	Number of Incidents	%	Function				
			Control	Alarm and Auto-Trip	Alarm	Record and Indicate	Affecting Propulsion
Burner Management	70	24.7					X
Miscellaneous	66	23.3					
Temperature	35	12.4		X			X
Alarm System	34	12.0			X		
Boiler Level	22	7.8	X	X			X
Flame Scanner	16	5.6		X			X
Superheat Temperature	8	2.8	X				X
F.D. Fan	8	2.8	X				X
Main Boiler Fuel Flow	7	2.5	X				X
Main Boiler Temperature Trip	4	1.4		X			X
Steam Pressure	3	1.1		X			X
Smoke Density	3	1.1				X	
Steam Flow	2	0.7	X				X
Fuel Oil Meter	2	0.7				X	
Ahead Steam Temperature	2	0.7				X	
Deaerator Level	1	0.4	X				X
Total	283	100.0					

TABLE IV-6

Types of Faults (Log #097)

	Number of Incidents
Circuit cards	95
Tranducers	83
Microswitches and relays	55
Solenoids	44
Complete Units	32
Miscellaneous	22
Timers	21
Mechanical	21
Power	12
Recorders and indicators	10
Controllers	8
Commissioning and design faults	4
Earth faults	3
Printers	3
Root extractors	1
Total	414

TABLE IV-7

Operational Vessel Failure Summary (Log #083)

Category	DIW	Reduced RPM	Other Obstruction	No Obstruction
Main engine system:				
Turbine blade and rotor, bearing, etc.	10	3	0	12
Maneuvering valve, governor, etc.	1	0	1	11
Main condenser	6	1	0	1
Boiler system:				
Boiler proper, boiler accessories	2	25	1	24
Main feed pump	2	0	0	10
Auxiliaries for boiler (fan, feedwater heater, deaerator, etc.)	5	10	0	27
Generator system (generator engine, generator)	5	0	0	37
Auxiliaries for engine	0	0	0	51
Refrigerators and air conditioners	0	0	0	16
Piping, valves and tanks	2	1	0	11
Instrumentation system (indicator, alarm, logger, etc.)	0	0	0	14
Electrical equipments	1	1	0	1
General equipments in engine room (crane, lathe, etc.)	0	0	0	8
Stern tubes	0	0	0	4
Subtotal	34	41	2	227

Log #066 also contains data on stops at sea and slowdowns per year. Table IV-8 tabulates this data. In the Log #066 data, the number of stops at sea was slightly less than those reported in Log #083, with the average of stops at sea being 0.67. However, at 3.34 slowdowns per year per ship, the average number of slowdowns per year was significantly higher.

B.(1)(f) Log #075

This paper documents a study to determine the length of the initial, or infant mortality, period for marine machinery. In addition, the study identified the causes of failures, and the contribution to total failure rates of various types of equipment. Data was collected on six turbine and four diesel vessels. All ten vessels had automated systems, and all of the turbine ships had two-boilers. Table IV-9 shows some of the statistics of interest related to the automated control systems.

As can be seen from the table, approximately 24 percent of the total steam vessel failures during the initial phase were due to the automated control system. Once the steady state, or so-called random period, was reached, the contribution to the overall failure rate by the automated controls on steam vessels dropped to approximately 17 percent. Converting this into failures per month per ship, the automated controls were experiencing on average 1.84 failures per ship per month during the initial period, and 0.56 during the random period. The highest contributor during the random period is piping and valves, which accounted for 53.9 percent or, on average, 1.82 failures per month during the steady state.

Because valves and valve controllers are often integral parts of the control system, some failures in this area would probably be classified as part of the control system as defined for the DOVAP study.

The conclusions of the study reported in Log #075 are as follows:

a) The time to reach the steady state condition varied from ship to ship, and the range was from three to eight months; however, the average time period was five months.

b) Major contributors to the failure rates were: (1) piping and valves; (2) automation equipment for turbine ships and main engine and deck machinery for diesel vessels.

c) Seventy-five percent of the initial failures were due to manufacturing, including bad installation, and defective workmanship.

TABLE IV-8

Failure Effect Data (Log #066)

	Stops at Sea	per Year	Port Delays	per Year	Slowdowns	per Year
	Number of Events	Number of Ships	Number of Events	Number of Ships	Number of Events	Number of Ships
Boilers	7	46	16	47	100	41
Condensate System	6	46	21	47	--	41
Main Turbine	6	46	--	47	--	41
Feed Pump	--	46	8	47	--	41
Other	12	46	15	47	37	41

TABLE IV-9

Relationship of Initial Failure Rate Period to Random Failure Rate Period and Major Contributions (Log #075)

Phase	No. of Failures	No. of Ship Months	Automatic Control Failures % of Total	Automatic Control Failures Ave. No. Per Month	Piping and Valve Failures % of Total	Piping and Valve Failures Ave. No. Per Month	Boiler Failures % of Total	Boiler Failures Ave. No. Per Month	Total Ship Machinery Per Month
Initial Phase;									
Steam Turbine;	552	72	24.1	1.84	21.6	1.66	12.5	0.95	7.67
Diesel;	248	48	10.2	0.53					
Random Phase;									
Steam Turbine;	415	123	16.7	0.56	53.9	1.82	3.4	0.11	3.37
Diesel;	255	100	27.1	0.69					2.55

d) During the random period, the major contributors to the unreliability were design defects and defects in materials.

B.(1)(g) Other Quantitative Data

In the data reviewed during Task I of the DOVAP study, a great deal of concern was expressed about boiler explosions, but no quantitative data was given. As explained in subsequent sections of this report, during DOVAP's performance of FMEA's and fault tree analyses, many conditions were found which could potentially result in an explosion. However, DOVAP found that usually a series of events must occur for an explosion to occur and that some of these events are outside of the automated control system.

In order to obtain an estimate of the actual frequency of boiler explosions, DOVAP combined data from two sources. The frequency of marine boiler failures was obtained from the ARINC Report, Log #508. Frequencies for commercial power boiler failures were obtained from a report generated by the National Board Members and Other Authorized Inspection Agencies for the year 1979.

The ARINC data reports failures on five classes of Navy steam turbine ships, and this data is summarized in Table IV-10. The mean boiler MTBF over all 5 ship classes is 2,320 operating hours. From the commercial power turbine data, as shown in Table IV-11, the percent of boiler failures due to explosions is 6.4. Using this percentage with the total failure rate of marine boilers from the ARINC data, the expected marine boiler explosions per million operating hours is 27.6. To convert this into expected explosions per commercial steam vessel with two boilers, it is first assumed boiler usage on average is 1.5 per day. This gives an accumulated usage of 13,140 operating hours per year per ship. Dividing the 13,140 expected boiler operating hours per year into the MTBF for boiler explosions of 36,232 hours, (i.e., the reciprocal of the 27.6 failures per million hours), gives an expected rate for boiler explosions of one every 2.76 ship-years. Although this is relatively infrequent, it is still frequent enough that it should be a major concern in the design and operation of automated propulsion control systems. This is especially true in view of the possibility of extreme damage to the propulsion system and, as indicated in Table IV-11, the possibilities of injuries or deaths to crew members.

TABLE IV-10

Log #508, ARINC Report; Boiler Failures Based 3M Data;
Mean Time Between Failure, Forced Shutdown

Ship Class	Number of Failures	Total Hours	MTBF (Hours)
1	86	66,261	728
2	43	85,982	1,999.6
3	19	220,262	11,600
4	74	134,280	2,228
5	25	66,261	2,650
	247	573,046	2,320

TABLE IV-11

Accidents Reported by National Board Members and
Other Authorized Inspection Agencies
(For the period January 1, 1979-December 31, 1979)

	Number of Accidents	Percentage of Accidents	Number of Injuries	Number of Deaths
Tube Rupture	281	23.1	2	
Shell Rupture	33	2.7	1	1
Furnace Explosions	78	6.4	13	1
Flarebacks	6	0.4		
Low-Water Failures	404	33.2		
Miscellaneous Overheating Failures	88	7.2		
Piping Failures	68	5.6	14	3
Poor Maintenance of Controls	73	6.0		
Unsafe Practice	23	1.9		
Construction-Code Violation (Welds)	1	0.1		
Dry Fired	102	8.4	2	
Tube-Sheet Crack	61	5.0		
Total	1,218		32	5

B.(1)(h) Information Received from Navy Maintenance Material Management (3M) System

DOVAP requested a special data run from the Navy 3M system on automated propulsion control systems failures that had been experienced on selected Navy ships. Data was requested on 16 ships which were known to have various levels of automation. The time period requested was from January 1981 through June 1982, or, a total of 288 ship months of data. Although this is probably the best data obtainable for substantiating predicted values, there are some limitations to the data, as follows.

Failure rates for individual component types cannot be computed because the quantities per systems are not known. In general, the complexity of the systems is considerably less than that of commercial systems. The data provided is for replacement parts, and it is assumed that the majority of the parts are requested because of failures. In compiling the statistics, expendable parts and materials were not accounted for, such as lamps and individual electronic parts (transistors, diodes, etc.).

The Equipment Identification Codes (EIC's) requested were for all failures recorded for automation control room components. No data was received related to valves, valve actuators, pneumatics and other hardware. It appears that the data included in this EIC classificatin is only for the control room electronic and associated field sensors. It is assumed that the printed circuit card failure rate is somewhat larger than the replacement rate because of the capability of the Navy to repair some circuit cards on-board. For the calculation of overall failure rates, DOVAP assumed that the equipment is on constantly, that is, 730 hours per month.

The ships covered in this study are presented in Table IV-12 and the summary data itself in Table IV-13. The summary shows that the Navy ships experience a failure every 1.6 months, for a mean time between failure of 456 hours (assuming 730 hours of operation per month). The top three contributors are: (1) switches, with a failure rate of .69 per month; (2) transducers/sensors at .48 failures per month; and (3) printed circuit cards with 0.19 failures per month. It is interesting to note that the switch failure rate is significantly higher than that for transducers and sensors. To date, much of the literature has emphasized the problems with transducers/sensors and relatively few documents note extensive problems with switches. Because switch problems can be just as critical as those of transducers/sensors, the application of switches should be scrutinized as severely as sensors and transducers.

Within the limitations cited above, there is a relatively close correlation between the predicted values from the DOVAP study and those from the 3M data.

TABLE IV-12

Ships Covered in 3M Special Data Run

JANUARY 1981 - JUNE 1982

AO-177	USS Cimarron
AO-178	USS Menongahela
AO-179	USS Merrimack
LKA-113	USS Charleston
LKA-114	USS Durham
LKA-115	USS Mobile
LKA-116	USS Saint Louis
LKA-117	USS El Paso
AE-32	USS Flint
AE-33	USS Shasta
AE-34	USS Mount Baher
AE-35	USS Kiska
DD-963	USS Spruance
DD-983	USS John Rodger
LHA-2	USS Saipan
LHA-4	USS Nassau

SHIP MONTHS = 288

TABLE IV-13

Summary Of Data From Navy 3M System

Overall MTBF = 456 Hours

	Type Total	Class Total	Failures Per Ship Per Month
1) Switches		199	0.69
2) Transducers/Sensors		139	0.48
RTD	69		
Transducers	11		
Sensors	6		
Pressure Transmitter	2		
Pick Up	1		
ARC Probe	30		
Probe	3		
Transmitter	5		
Level Indicator	6		
Flow Transmitter	1		
Pressure Transducer	4		
Diff Pressure Unit	1		
3) P.C. Cards		56	0.19
4) Indicators		29	0.10
5) Amplifiers		17	0.06
6) Ignitors		6	0.02
7) Meters		5	0.02
8) Alarms		3	0.01
9) Tachometers		3	0.01
10) Buzzer/Siren/Horn		3	0.01
11) Supply		3	0.01
TOTAL		463	1.60

B.(2) R&M Qualitative Data

About sixty documents reviewed during Task I literature survey contain qualitative R&M data of some type. This ranges from complete methodology papers to detailed descriptions of problems incurred in service, to "nuggets" which cite a particular failure mode, trend, reliability design precaution, or the like. The major findings and conclusions in the area of qualitative R&M data can be summarized as follows:

B.(2)(a) Failure Modes and In-Service Experience: These two areas are related because in-service experience quite often involves detection and/or correction of failure modes. A considerable amount of data is provided. This includes:

a) There is general concensus that sensors appear to present one of the biggest "inherent" reliability problems.

b) Many premature failures occur in automation systems, and a large percentage of these stem from shipyard installation. Many wiring error problems were cited. Also, many operational problems with pneumatic and hydraulic systems were encountered due to dirt, moisture and leaks induced during construction. One study (Log #026) reports a correlation between achieved reliability and the shipyard constructing the vessel. The author attributes this to the quality control (or lack thereof) exercised during manufacture and installation.

c) Several papers report that "small" items (sensor, remote valve operators, limit switches, etc.) cause more problems than does major machinery. One paper, however, (Log #053) reports that there are indications that machinery faults prevent unattended engine room operation more often than control and instrumentation faults.

B.(2)(b) R&M Methodology: Several documents describe methodologies for reliability and maintainability analyses. Some of these tend to be overly tutorial, or else too specific for general application. Only one document, Log #070, which is in textbook format, was found that could be utilized effectively by someone without an extensive R&M background.

B.(2)(c) Maintenance Practices: Most of the documents that dealt with maintenance practices were developed for the Navy, but all documents that addressed this topic cited the correlation between good maintenance practices and good reliability. Only five formal maintenance systems, other than Navy systems, were reported. One of these was the system

evaluated on the M.V. Sugar Islander.

The Sugar Islander "system" consisted of a program of scheduled maintenance and reporting, with emphasis on preventative maintenance. It is reported that this system reduced costs, permitted better inventory control, and facilitated the detection of impending failures.

In all these documents, there was general agreement that with engine room automation, watchstanders could devote more time to maintenance. It was not conclusive, however, that this time was used for preventative maintenance. Several papers reported that the automation system itself required considerable maintenance, with one paper reporting that this required two to six hours per day for testing, adjustments, and servicing. Also, wth steam systems, it appears that a considerable amount of time is spent "fine tuning" the system. Several papers point out that when done properly, this reduces operating costs. It was also pointed out that this increases reliability. (For example, burning with low excess air improves the boiler operating environment.)

B.(2)(d) Design Approaches for Reliability: A number of papers at least touched on this subject. These primarily dealt with redundancy provisions, back-up power supplies, sensor mounting approaches, etc. Conflicting views were given with respect to the reliability of signal multiplexing onto a single cable versus individual signal cables. All in all, however, the few in-depth treatments of this subject were primarily Navy-related.

B.(3) Maritime R&M Status Information

Four documents contain specific information on the status of R&M in the maritime industry; a number of other documents make points related to this topic. The most comprehensive document reports on a study of maritime R&M status done for MarAd (Log #116). This study was done in 1976, and nothing comprehensive and more recent was found during this literature search. This document concludes that (1) an R&M program is needed in the maritime industry, (2) an R&M data base is needed, and (3) that more attention should be devoted to environmental factors. DOVAP feels that this document and its conclusions are still valid.

In 1977, a study was conducted for MarAd to initiate an R&M program (Log #047). The study reported in Log #047 was the first phase of the program, and recommended three subsequent phases, viz (1) development of a pilot program, (2) implementation of the pilot program, and (3) implementation of the continuing program. No subsequent information concerning the fate of this program was found during this literature

search.

A number of documents cite the need for a maritime R&M program, and the problems that would be involved. The need for an R&M data base is often mentioned. The need for more R&M analyses is also cited. Problems mentioned with respect to R&M analyses include the lack of a high population of common equipment, which could impact statistical validity. Also, the environmental spectrum differs considerably from ship to ship so that the reliability of identical equipment on different ships could vary. DOVAP also noted that the definition of failure varies widely. In some cases, failure is defined to mean only loss of ship operating time, in other cases to mean the need for corrective maintenance.

The status of R&M in the Navy, of course, involves a highly developed discipline. One of the Navy's more recent R&M approaches, which could have applications in the commercial field, is the engineered operating cycle. The basis of this approach is to evaluate historical maintenance experience in order to identify areas/items requiring attention. This "attention" can consist of overhaul tasks, improved training, the acquisition of more reliable hardware, etc. Significant cost savings can accrue through this approach because low-reliability items are weeded out, overhaul schedules are lengthened or overhauls eliminated if historical data indicates this is feasible, etc.

B.(4) Automation Configuration Information

About fifteen documents provide information on the hardware configurations and system/subsystem layouts of engine room automation, and contain good hardware descriptions of current and proposed systems. These documents can supplement more detailed and specific system documentation (e.g., schematics, logic diagrams) during R&M analyses.

B.(5) Automation State-of-the Art

About fifteen documents provide information on the state of the art of engine room automation specifically, and maritime automation in general. These documents primarily discuss instrumentation and microprocessors/computers. Overall, it appears that maritime automated control systems have not evolved as fast as the existing technology. This could be due to owners/operators feeling that state-of-the-art controls are not cost effective.

The literature search indicates definitely that the cost effectiveness of computer systems has not been established. This is because, in part, standardization of computer systems is difficult, and software is a high risk and costly item. A few

papers recommend that software be developed concurrently with the hardware, but overall, software considerations were conspicuous by their absence.

Some on-board computers have exhibited excellent availability (up to 99 percent). This is attributed to redundancy provisions, self-check features, adequate spares available for repair, and modular design approaches for ease of component replacement. Other features cited as desirable include provisions for system check-out, adequate diagnostic routines, "fail gracefully" system architecture, and immediate failure response to protect against secondary failures.

In the area of instrumentation, sensors are cited as a major "weak link" in system reliability. Some sensor problems are due to poor application, primarily in that the sensors were not developed for marine use. Other problems are due to poor installation (workmanship) and poor maintenance.

A "learning curve" in the operation of automated systems is readily apparent. False alarms are reported to be a big problem during the first two years of operation. It is also reported that the frequency of alarms, both real and false, decreases over the first two years. One study shows that after a "steady state" is reached, there is an average of one real alarm every three days and three false alarms per month. Another document reports that after de-bugging, alarms are rare, and that alarms at night on the order of one per month, or less, are not unusual.

Most documents do not address the consequences of alarms, e.g., the downtime due to real and false alarms, the time spent switched over to manual, whether the cause of the alarm was corrected through repair or fine tuning the system, etc. The need for better and more frequent sensor and systems checks is cited.

B.(6) Spare Parts Assessments

About ten documents discuss spare parts provisioning or assess spare parts policies. These documents generally concur that provisioning policies are ineffective and haphazard, and that the shipboard spares status is generally unknown. A particularly comprehensive assessment of spares policies (Log #005) reports that spare parts provisioning levels were based on subjective experience which tended, in many cases, to be greatly influenced by recent equipment failures. This document also reports that in spite of poor spares policies there were few sailing delays due to temporary repairs, loans, and substitutions, and because suppliers often maintained depots in key areas. Another document (Log #011), however, reports that sections of automation systems were out of service for months due to lack of spare parts. Also, one of the contributing

factors cited in the investigation of the ramming of the Lorenzo D'Amico by the China Sea (Log #007) was lack of spare parts for the engine control system.

B.(7) Regulations/Requirements

About ten documents provide information on mandatory and non-mandatory regulations and requirements. These include the regulations documents themselves, such as the USCG "Navigation and Vessel Inspection Circular No. 1-69, Subject: Automated Main and Auxiliary Machinery," the ABS Rules for Building and Classing Steel Vessels, MarAd standard specifications, and the IEEE Recommended Practices for Shipboard Installations. They also include a few papers that discuss the regulations.

None of these regulations/requirements specify quantitative R&M provisons. Numerous qualitative requirements to enhance R&M are in evidence throughout all of them. There is some overlap in qualitative requirements among these various documents,but in many cases each document specifies requirements that the others do not cover.

Each document contains specifications for the operating environment the equipment must withstand. This includes temperature, shock, vibration, acceleration, etc. The requirements vary from document to document as illustrated in Table IV-14.

B.(8) Environmental Information

About thirty documents provide environmental information of various types. The subjects covered include vibration, materials compatibility, corrosion, shipboard EMI, and the shipyard environment. Other documents also cite various aspects of the shipboard environment, ranging from dust (grain ships) to vapors and battery fumes, and even to spilled beer.

In the areas of vibration and materials compatibility, the emphasis is almost entirely on hulls and structures. Except for an occasional mention, such as the need for shock mounts or the need to protect dissimilar mating materials, considerations in these areas for automation equipment were conspicuous by their absence.

Vibration is recognized as a big problem, especially in recently built ships, but its relationship to reliability, in general, does not seem to have received much attention. One document (Log #029) summarizes the state of the art of vibration analysis and prevention, and points out that there are controversy and conflicting views, and that a major, long-range effort is still required to fully understand the underlying phenomena and provide design tools. There is general agreement

Table IV-14

Environmental Specifications

	MarAd standard spec. for Merchant ship construction	MarAd standard spec. for Diesel Merchant ship construction	ABS rules for building and classing steel vessels	IEEE recommended practice for electric installations on shipboard	U.S.C.G. NVIC 1-69
Temp.	Engine room/boiler room: $0^{o}C$ to $50^{o}C$ Areas outside Engine room/boiler room: $0^{o}C$ to $40^{o}C$	Ambient temperatures up to $50^{o}C$	Semiconductors interior compartments; $0^{o}C$ to $50^{o}C$ inside consoles; $0^{o}C$ to $60^{o}C$	Open decks/ bridges: $-40^{o}C$ to $+55^{o}C$ Engine room: $0^{o}C$ to $+65^{o}C$ Outside of Engine spaces; $0^{o}C$ to $40^{o}C$ Storage: $-40^{o}C$ to $+70^{o}C$	Not specified
Vibration	5 to 15 Hz, 0.030" + 0.006" amp. 16 to 25 Hz, 0.020" + 0.004" amp. 26 to 33 Hz, 0.010" + 0.002" amp. +30 roll, 8 seconds min, 30 second max +10 pitch, 6 seconds min. 25 seconds max +1g: transverse +0.5g: longitudinal +1.5g: vertical	5 to 15 Hz, 0.030" + 0.006" amp. 16 to 25 Hz, 0.020" + 0.004" amp. 26 to 33 Hz, 0.010" + 0.002" amp.	2 to 13.2 Hz, 0.08" peak to peak amp. 13.2 Hz to 80 Hz, at 0.7g accel. 30 inclination from the vertical, any axis	1 to 4 Hz, 0.4" amp. (peak to peak) 4 to 8 Hz, 0.1" amp. (peak to peak) 8 to 14 Hz, 0.03" amp.(peak to peak) 14 to 30 Hz, 0.01" amp. (peak to peak) 30 to 100 Hz, 0.002" amp. (peak to peak)	Not specified

that vibration is a function of many variables (such as ship speed), and that vibration levels for a particular ship often remain unknown prior to actual operation.

In the area of corrosion, several papers point out that electrical/electronic components used on board a ship may not have been designed for the marine environment. Protective measures recommended include use of hermetically sealed or conformal coated electronics components, use of moisture proof connectors, plating of metal parts, etc.

Shipboard EMI is another area recognized as a big problem. One paper (log #021) reports that transients as high as 600 to 700 volts have been measured on common supply lines. Another paper (Log #034) reports extensive problems due to electronic components being damaged by electrostatic discharge, even in the high humidity of the shipboard environment. Several other papers report high RFI and EMI in engine rooms and on bridges. Still, few practical approaches to the control or prevention of EMI are discussed except for recommendations in Log Numbers 021 and 034. The regulations/requirements documents specify some provisions, such as grounding, use of twisted pairs in certain cases, etc. It is not clear that these are specific and in-depth enough, however, for the modern, shipboard electronic environment.

The effect of the shipyard environment on reliability was discussed in SectionB(2)(a) above, where it was pointed out that many premature failures in automation systems stem from shipyard installation. One paper (Log #026) reports a direct correlation between the shipyard constructing the vessel and the vessel's casualty rate. Several papers cite "dirty" shipyard conditions as the cause for later reliability degradation.

B.(9) Other

Several topics are included under this heading and are discussed below.

B.(9)(a) Condition Monitoring/Failure Prognosis: Ten documents were obtained (out of many available) on this subject. Two of these (Log #058 and #112) described VIDEC, the vibration and thermal analysis system evaluated aboard the S.S. President Johnson. Other documents describe new trends or applications of existing conditon monitoring approaches. Two documents report "successes"; one (Log #054) with the Navy's use of ferrographic lube oil analysis, and another (Log #028) with pre-dry dock equipment vibration surveys.

Overall, this area appears to still be in its infancy, and reports generally seem inconclusive as to the benefits of condition monitoring. Each system is unique in terms of the signatures it generates for use in condition monitoring, and it can take years to reach a steady state condition. In addition, most equipment tends to degrade with time, and the ship vibration spectrum can also be constantly changing. Such factors as these create problems with establishing a baseline for accept/reject failure prognosis criteria.

B.(9)(b) Data Bases: Seven documents discuss this topic, and there is agreement that except for Navy data, existing U.S. maritime data bases are not adequate for reliability and maintainability quantitative evaluations. Existing non-Navy data bases, such as those maintained by MarAd and the U.S.C.G., do not provide operating time, reports on all equipment that failed, nor the number of equipments that did not fail. One document reports that the private sector often considers their data proprietary. To overcome such problems, and to permit numerical evaluations based on actual, operational data, many documents cite the need for a standard, R&M reporting system.

B.(9)(c) Crew Skills/Training: About fifteen documents specifically address crew skills and/or training, and a large percentage of all documents make some reference to this area. DOVAP noted that often the need for better training was used as a sort of "cure all" conclusion, and that there was little further discussion as to the specific training needed.

One document generated for the Navy pinpointed a problem due to the lack of analog troubleshooting skills, and recommended training in this area. Less specific recommendations in other documents involve the use of training simulators, union schools, and on-board cassettes and video tapes.

There is general agreement that human factors in the maritime industry need attention. One study reported that 25 percent of all control system adjustment or calibration problems were caused by the crew. Several papers reported that maintaining and troubleshooting an automation system were beyond the capabilities of the crew. A reason given for this was that the uniqueness of each system and the crew turnover rate did not permit personnel to become familiar enough with the equipment. A few papers recommended that an "electro-technician" be added to the regular on-board crew.

The Maritime Transportation Research Board recently identified critical issues in need of examination (Log #068). Due to the increase in vessel accidents of all types, one of these issues was maritime safety. The Board stated that extensive efforts have been taken to alleviate this problem, and

that the emphasis has been on physical solutions (design, construction, etc.). It is pointed out that the most serious aspect of the safety problem involves people. The nebulous nature of the problems to be solved is also pointed out, and the urgent need for research on personnel is cited.

B.(9)(d) Support Equipment/Documentation: This category involves the "back up" required to operate an automation system and keep it running, and includes test equipment, maintenance manuals, troubleshooting procedures, and the like. Six documents were found which made reference to this area, but overall, these subjects were conspicuous by their absence.

The need for better fault isolation and check-out procedures was cited, as was the need for adequate test points on printed circuit boards. One paper describing experience with a computer-based system reported that diagnostic tapes were available, but that when the computer malfunctioned it was not possible to read-in the tapes. Another reported high availability of a computer system, with one of the reasons being that problems had not occurred which precluded reading-in of the diagnostic tapes.

The literature search indicates to DOVAP that this is an overlooked area, and is in need of attention. While often simply a nuisance or shortcoming, lack of adequate support equipment and documentation can lead to a hazardous situation. One of the contributing factors cited in the ramming of the Lorenzo D'Amico by the China Sea (Log #007) was lack of troubleshooting and repair procedures for the engine control system.

V. CONTROL SYSTEMS SELECTED FOR REVIEW

During Task II, the engine room automation systems on two steam vessels and one diesel vessel were analyzed. For these analyses, three major overall criteria were established.

The first major overall criteria of the study was that the systems evaluated represent different technological approaches. To this end, the Coast Guard selected the particular vessels to be analyzed from a candidate list of vessels developed by DOVAP.

The second major overall criteria was that each system be evaluated to the same depth of detail. To accomplish this, DOVAP obtained documentation that would permit analysis down to the detailed circuit level on all three systems. This documentation consisted of circuit schematics, parts lists, wiring diagrams, panel layouts, and various types of technical manuals.

The third major criteria involved establishing system boundaries, or, in other words, defining where the engine room control system "stopped" and other ship systems "began." The ground rule applied in defining these boundaries was based on whether or not the vessel would be fitted-out with the equipment in question if it did not have an automated control system. Based on this ground rule, support systems such as ship's electrical power and control air were deemed not a part of the systems to be evaluated since they would be provided on-board regardless of whether the engine room was automated. Other areas ruled out by this ground rule were atomizing steam, gland steam, pumps (fuel pumps, lube oil pumps, etc.), and valves not specifically required by the automated controls.

In the subsections that follow, the vessels and their control systems selected for review are described. Various other aspects of study coverage and ground rules are also discussed for each of the three vessels. These aspects are those that are applicable to all Task II reliability analyses. Aspects unique to a particular Task II effort (e.g., predictions) are discussed in the section devoted to that particular effort.

A. CONTROL SYSTEMS SELECTION PROCESS.

Considerable effort was devoted to the selection of the control systems that would be investigated during the study. DOVAP generated a list of candidate systems based on the following criteria:

a) The vessel must have an automated propulsion control system.

b) The candidate vessel should have been handed over to the

owner/operator within the last five years. This was to ensure that the system is of the current state of the art, and also that there is susbstantial operating time on the vessel.

c) The vessel is in excess of 1600DWT.

d) The vessel has been operated beyond the various warranty periods.

e) The vessel is a U.S. flag.

f) The control system is produced by a U.S. manufacturer

g) Sufficient documentation on the vessel is available for analysis during the study period.

The objective of this portion of the study was to provide a candidate list to the Coast Guard based on the above criteria. The final selection of the systems was made by the Coast Guard during the first workshop. During the preliminary investigation, shipyards confirmed that the types of control and monitoring systems installed in various vessels were usually defined in the initial ship specifications. The ship yard, in turn, obtained bids from various control system manufacturers, and based the selection of the control system subcontractor upon these bids. In some cases control system manufacturers had been able to have their systems defined within the body of the specifications. The investigation also revealed that the number of companies offering complete systems of their own design is limited.

Based on the process just described, three vessels were selected for analysis. Two of them (Ships A and B) are steam-driven, and one (Ship C) is diesel.

B. SHIP A CHARACTERISTICS, COVERAGE AND GROUND RULES

B.(1) Ship A Characteristics

Ship A is a 165,000 DWT turbine tanker, and is one of six ships of its class. It was delivered in the summer of 1979. Its regular trade route takes it from tropical to subartic regions, with each voyage taking about one month. Most of each voyage is spent in the full ahead cruise mode, with maneuvering requiring roughly 15 hours per voyage.

It has two boilers, with three burners per boiler. A two-man engine room watch is maintained at all times.

Ship A contains two essentially separate automation systems with only a small amount of interfacing between them. These

were built by two different manufacturers, and one system provides automatic boiler and combustion control while the other provides turbine speed and direction control. Each system has two manual back-up modes.

B.(2) Ship A Boiler and Combustion Control Characteristics

The boiler and combustion control system on Ship A is based on a hybrid digital-electronic/pneumatic approach. The purge and light-off sequence, boiler and burner trip control, and the alarm/annunciator system are implemented with digital logic. Pneumatic control loops are provided for such parameters as superheated steam temperature, fuel oil and combustion air flow, fuel oil temperature, etc. Some relay logic is used for feed-pump control and automatic burner sequencing. In addition, the manual back-up boiler front panel is extensively implemented with relay-based control. Essentially no electronic analog controls are utilized.

Automatic sequencing of a boiler's three burners allows selection of a base burner, which remains lit, and automatic on/off control of the other two burners to match increases or decreases in steam demand.

Boiler and combustion control can be exercised in three ways. In the automatic mode, control is from the engine room console (ERC), which provides completely automatic sequencing and safety shutdown. In the manual back-up mode, control is from the boiler front panel. This mode provides complete boiler control but contains no boiler safety or trip features. The third mode is totally manual and requires manual opening/closing of valves, inserting/retracting of ignitors, etc. There are no provisions for boiler or combustion control from the bridge.

Four conditions cause a boiler trip in the automatic mode, namely:

a) Boiler drum level below low-low

b) Loss of combustion air (fan fail)

c) Purge or light-off sequence fail

d) Burner trip (burner valve open and no flame)

Any of these trip conditions causes the boiler master fuel oil valve to close. In addition, light-off is inhibited if any of these conditions exist.

There are two identical sets of boiler controls, one for boiler #1 and one for boiler #2. In addition to the actual control devices, a number of alarm/annunciators is provided for both boilers.

B.(3) Ship A Turbine Speed and Direction Control Characteristics

Ship A's automatic turbine speed and direction control is based on a classical, feedback servo loop. Signals from the bridge or engine room throttle lever are compared with the actual positions of the ahead and astern steam valves. A signal proportional to the error between the commanded and actual positions is thus continuously generated. This error signal drives a slide block in a hydraulic manifold such that the requisite hydraulic pressure is applied to increase or decrease the opening of the turbine ahead or astern steam inlet valves.

The feedback servo loop extensively utilizes electronic-analog circuitry. The hydraulic portion of the system is based on a variable displacement hydraulic pump.

Two manual back-up modes are available. First, a manual hydraulic handpump is provided so that hydraulic pressure can be maintained in event of failure of the variable displacement pump unit. In the handpump mode, there are also manual provisions for opening/closing the turbine steam valves. This is accomplished through an ahead/astern selector switch coupled with a manual control valve for adjusting opening/closing rates for the turbine steam valves. This latter provision enables manual speed and direction control in event of failure of the automatic servo control loop.

In the second manual back-up mode, speed and direction control is achieved by direct, manual operation of the turbine steam valves via their valve spindles. This operating mode would be used in event of complete failure of the hydraulic system.

In the automatic operating mode, nine conditions can cause a turbine trip, namely:

a) Turbine lube oil pressure low

b) Turbine vibration high

c) Condenser level high/low

d) Boiler steam pressure low

e) Turbine overspeed

f) Turbine steam valve overtravel

g) Boiler drum level high

h) No auto rollover when throttle at stop

i) Hand turning gear engaged in auto mode

Any of these trip conditions, as well as manual depression of the trip pushbutton, cause the turbine steam valves to close. The only interfaces between the boiler control and turbine control systems consist of the boiler steam pressure and drum level signals needed for the above trips. There are no turbine trip provisions in the manual modes.

As indicated above, automatic turbine control can be exercised from either the engine room or bridge, depending on which location is in control. Control location selection switches and indicators are provided on both the bridge and engine room consoles, as are turbine trip pushbutton switches.

An extensive turbine alarm/indicator array is mounted on the engine room console. Four turbine system alarm indicators are mounted on the bridge console, namely:

a) Throttle control manual trip

b) Shaft stopped

c) Throttle control off normal

d) Throttle control hydraulic pump failed

B.(4) Ship A Coverage and Ground Rules

The Task II analyses of Ship A covered all automatic controls for the boilers, steam plant, and turbine. This coverage extended down to the part level (e.g., integrated circuit gates and flip-flops, relays, pneumatic control valves, etc.).

Parts were grouped functionally for analysis where the parts within the group exhibited the same failure effects. For instance, the electronic parts constituting a solenoid driver were combined into a solenoid driver functional grouping on the basis that the failures of any of these parts would cause the solenoid driver to either stay active or stay inactive.

All electronic parts were assumed to be constantly powered. Also, it was assumed that no preventative maintenance is possible for electronic parts. Both these assumptions are realistic.

The analyses covered only hardware needed for automatic operation. Manual back-up provisions were not specifically considered although they were evaluated and included in two cases. These cases are (1) where failures in manual back-up equipment can interfere with automatic operations, and (2) where specific hardware is common to both the manual and automatic modes. This commonality occurs on Ship A in some areas of the

boiler front panel where equipment in this panel serves interface functions between the boiler and the engine room console for sensors and switching.

Light emitting diodes are provided on many electronic printed circuit cards for troubleshooting purposes. These indicators were not considered in the analyses.

The ship's auxiliaries were not considered. These were excluded primarily on the basis of the overall ground rule cited above involving whether or not the equipment would be provided if there were no automation. In some instances, there is automation associated with the auxiliaries (alarms, pump off/on controls, etc.). In these instances, however, there is no interface of any type with the propulsion system automation.

On Ship A, communications equipment ranges from the ship's telephone system to sound powered telephones and walkie-talkies. These were not considered during the analyses because the overall communication system appeared adequate for any need that might arise due to engine room automatic control failures.

Finally, the engine room console power supplies were considered only at the "black box" level during the Task II analyses. These power supplies consist of two redundant units for converting the ship's AC power to the DC needed by the controls. They are purchased as off-the-shelf units from a power supply manufacturer. They were considered at only the "black box" level for two reasons. First, since they are redundant, potential reliability problems should have been minimized. Second, as off-the-shelf units, their design adequacy should have been proven.

C. SHIP B CHARACTERISTICS, COVERAGE AND GROUND RULES

C.(1) Ship B Characteristics

Ship B is a 39,990 DWT turbine tanker, and is one of three ships of its class. It was delivered in September of 1981. Its regular trade routes are the west coasts of the United States and Mexico. Length of time of voyages varies from three to fourteen days. The maneuvering time in and out of port varies anywhere from two hours to twenty hours. The normal watch during cruising is one unlicensed watchstander and one engineer. The vessel contains two boilers and two burners per boiler. During maneuvering and normal cruising usually both boilers and both burners are on. When the ship is tied up, usually one burner per boiler is on.

C.(2) Ship B Control System Characteristics.

The automated controls on Ship B are provided by two major manufacturers. One supplies the controls for the boiler and the majority of the auxiliaries, the other supplies the controls for the turbine. The turbine controls are the same as on Ship A.

The boiler controls and auxiliary controls utilize a combination of analog and digital electronic circuits. The analog control circuits automatically monitor and control continuously changing system values. Each control circuit is provided with a manual automatic station or selector switch to permit manual control of individual valves and dampers when conditions demand a remote/manual mode of operation.

The boiler control analog circuits covered in this study are:

a) Deaerator level control.
b) Combustion control.
c) Superheated steam temperature control.
d) Feed water pump differential pressure control.
e) Drum level control.
f) Feed water recirculation valve control.
g) Steam dump control.
h) Fuel oil temperature control.
i) Fuel oil recirculation control.

Digital controls provide on/off, and in some cases automatic sequencing for individual pieces of equipment. The digital circuits covered in this study are as follows:

a) Lube oil service pump switching.
b) Feed pump start/stop circuits.
c) Burner management subsystem.

The digital control circuits for the lube oil service pumps and the feed pumps automatically switch-in the standby unit upon primary pump shutdown. The burner management controls provide automatic light-off and the safeguards for automatic burner and/or boiler shutdown.

C.(3) Ship B Coverage and Ground Rules.

The study coverage and ground rules applied to Ship B are the same as those for Ship A.

D. SHIP C CHARACTERISTICS, COVERAGE AND GROUND RULES

D.(1) Ship C Characteristics

Ship C is a 27,500 DWT twin-diesel tanker and is one of nine of its class. It was delivered in 1975. It is chartered as a supply vessel, and operates on a tramp route worldwide. Maneuvering requires roughly 20 hours per month, with the remainder of the time spent in the full ahead cruise mode. Its two 7,000 hp diesels drive a controllable pitch propeller (CPP). Ship electrical power is from a generator driven by the main shaft.

Ship C's automation system provides both engine and CPP control. There are three modes of operation: (1) cruise mode in which the engine room is in control and trims shaft speed to meet the requirements of the shaft driven generator; (2) maneuver mode in which either the bridge or engine room can exercise control via their respective throttle levers; and (3) split mode in which the engine room exercises direct, operator control of each of the two engines. In the maneuver mode, the engine room normally exercises control when waterway restrictions dictate quick response. When such restrictions do not exist, the bridge maintains control during maneuvering. A local control station between the two engines two levels below the engine control room provides manual back-up capability.

A one-man engine room watch is maintained during normal cruising. A two-man watch is provided while maneuvering.

Ship C's control system consists of four functional areas. Each of these is discussed below.

D.(1)(a) Station in Control

Since the vessel can be controlled from either the bridge, engine room, or local station, "station in control" logic is provided. This logic is implemented with digital electronics, and performs two functions.

The first function is to control and sequence transfers of vessel control from one location to another. The second function is to generate the "station in control" signals which enable or inhibit, as appropriate, vessel control commands from each of the three control locations.

D.(1)(b) Engine and Clutch Control

The engine and clutch control function is primarily implemented with digital logic, and controls stop/start and clutch/declutch of each engine. A number of permissives are involved in these processes. For instance, engine start is

inhibited if engine lube oil pressure is inadequate; the engine is inhibited from being clutched in until it has come up to speed.

This control area also provides engine safety shutdowns. These occur if any one of the following eight parameters are out-of-limits:

a) Engine lube oil pressure

b) Fuel oil pressure

c) Rocker lube oil pressure

d) Jacket water pressure

e) Jacket water temperature

f) Injector coolant pressure

g) Injector coolant temperature

h) Reduction gear lube oil pressure

A manual override is available to prevent engine shutdown from any of these eight conditions. A ninth shutdown condition--engine overspeed--cannot be overridden.

D.(1)(c) Mode Control

The mode control function utilizes both analog and digital circuitry to route vessel speed and direction commands from the appropriate controlling device (e.g., bridge throttle lever) to the pitch and engine speed controls. The initial step in this routing is governed by the setting of the mode switches, i.e., cruise, maneuver, or split mode.

Depending on the mode selected, and whether one or both engines are on-line, the mode control logic selects an appropriate function generator (e.g., 1-engine cruise mode, 2-engine maneuver mode, etc.) and connects it via relay contacts with the output of the controlling device. These function generators utilize analog circuitry to translate the signal from the controlling device into non-linear functions representing operating curves of the speed and direction commands.

D.(1)(d) Pitch Control

Propeller pitch control is achieved by a classical, feedback servo loop. Pitch command signals from the function generators are continuously compared to a signal representing actual pitch, and an error signal is generated. The error signal

is sent to the CPP where it is utilized by a hydraulic unit to effect changes in propeller pitch. Pitch control circuitry also controls the rate at which pitch is changed.

Propeller pitch control is primarily implemented with analog circuitry.

D.(2) Ship C Coverage and Ground Rules

The Task II analyses of Ship C covered all engine and pitch controls. This includes all four functional areas described above. This coverage extended down to the part level (e.g., integrated circuit gates and flip-flops, relays, etc.).

As with Ships A and B, parts were grouped functionally for analysis where the parts within the group exhibited the same failure effects. For instance, the parts in the pitch control summing amplifier were considered a functional grouping because their individual failures would cause either loss of the amplifier output or a constant, incorrect output.

The communications system on Ship C was not considered. It was reported to be extensive, but only very scanty specific data was available on it, so its adequacy cannot be assessed.

Ship C has a microprocessor-based bell logger. Since this unit is used strictly for bell logging and does not have an interface with propulsion system controls, it was not considered in the analyses.

VI. FAILURE RATE PREDICTIONS

The validity of much of the work associated with the FMEA's, the criticality analysis and the fault trees depends on good estimates of part failure rates. Because of the importance of obtaining good estimates of commercial vessel control system failure rates, every available source of failure rate information was used. The following subsections describe the data sources and how the data was used to obtain the failure rate estimates for part classes and types.

A. FAILURE RATE SOURCES

The following data sources were scrutinized for failure rate information and failure mode data applicable to this study.

a) "Electronic Equipment Reliability Data," published by Reliability Analysis Center, Rome Air Development Center (RADC), Fall 1980. This publication is a summary of equipment level reliability data on military electronic equipment. The data summarizes reliabilities at the subsystem, group, and unit level. Approximately 94 percent of the equipment covered in this report are used on military aircraft, 4 percent for ground application, and 2 percent for shipboard application. The reliability data was essentially obtained from contractually deliverable documentation associated with reliability data, such as Air Force AFR66-1 and Navy 3M data collection systems.

b) "Nuclear Plant Reliability Data System, 1980 Annual Reports of Cumulative System and Component Reliability." This report was prepared by the Southwest Research Institute (SRI) and published in September, 1981. These annual reports were designed to serve as a source of reliability and failure statistics for operators, designers, manufacturers, and regulators of nuclear power plant safety-related systems and components. These reports provide operating statistics of safety-related systems within a unit which may be used to compare and evaluate reliability performance. The reports also provide failure mode and failure rate statistics on components which may be of use in failure modes and effects analysis, fault/hazard analysis, and probablistic reliability analysis.

The data in these reports cover the period between July 1, 1974 and December 31, 1980 and contain reliability data on approximately 4,000 different types of components within 25 subsystems. This is an excellent source of data because the total operating

hours down to the component or part level are usually in excess of millions of hours. In addition to failure rate data, the report summarizes how failures were detected, the application of the units, and the status of the system when the failure was detected. For each failure mode and total part failure rate the rates are calculated for the minimum, 25th percentile, median, 75th percentile, and maximum values for each failure mode and for the total of the parts. The percentiles were computed by the methods suggested by Conover (1).

c) "Nonelectronic Parts Reliability Data," published by Reliability Analysis Center (RAC), Rome Air Development Center, Summer 1981. This data summary provides failure rates and some failure modes information for mechanical, electro-mechanical, electrical, pneumatic, hydraulic, and rotating parts. The data utilized in the development of the publication was collected by RAC, and presents equipment level experience in military, industrial, and commercial applications. In the calculations of these statistics, it was assumed that the failure rates of nonelectrical parts follow the exponential distribution. That is, the parts display a constant or random failure rate. Based on this assumption, the mean and 60 percent confidence intervals were calculated.

This report includes equipment failure rates for practically every environment, e.g., dormant, satellite, ground fixed, airborne, helicopter, ship environment, submarine environment, etc.. In many cases, the total operating hours for individual parts are well over millions of hours. The report also provides some failure mode information and was used as back-up information for obtaining the failure mode breakdowns used by DOVAP in this study.

d) "Missile Systems Division, Reliability Engineering Manual," published by Lockheed Missile and Space Company (LSMC), 1 August 1963. This volume contains generic failure rates for electrical and mechanical components. Upper and lower confidence levels are given for the failure rates of each component type. The upper and lower limits correspond approximately to the 3σ limits of the normal distribution. Because the

(1) W.J. Conover, Practical Nonparametric Statistics, New York, John Wiley, Inc., 1971.

data is comparatively old, DOVAP did not include the failure rates in the overall calculations of the adjusted failure rates for ship applications. Rather, the failure rates were regarded more as a checkpoint to determine if ballpark figures correlated.

e) "Government-Industry Data Exchange Program (GIDEP). Volume Reliability, Maintainability Analyzed Data Summaries," latest volume published July 1981 with updates included as of September 1982. The GIDEP reliability and maintainability data bank includes information on failure rates, failure modes, replacement rates, mean time between failures, and mean time to repair on parts, components, equipments, subsystems, and systems. This source includes data from field experience, laboratory accelerated life tests, and reliability and maintainability demonstration test results. In addition to the summarized information, GIDEP provides microfilm reports on individual back-up data.

The failure rate data and replacement rate data are statistically analyzed and presented in the form of group 99 percent confidence intervals with a mean value for each major subject category. The 99 percent confidence interval is calculated for failure rates for each part type. The data is grouped by major subject categories, part number listing, and by vendor listing. Because of the extensive participation in the GIDEP program by most military contractors, a wide range of environments and a large accumulation of test and operating hours are covered.

f) "Establishment of Reliability and Maintainability Data Bank for Shipboard Machinery," published by ARINC Research Corporation, dated March 1973. This report presents summaries of failure rates and maintenance rates for Navy shipboard machinery. Little information is reported for control system components; however, some useful failure rate information is given on valves, pumps, and boilers. The source for this information is the Navy's 3M system, and where sufficient data is available, 90 percent upper and lower confidence levels are calculated.

g) "Storage Reliability of Missile Materiel Program," published by Raytheon Company, May 1976. This report summarizes and analyzes the non-operating reliability of missile materiel. However, as a comparison the report also develops operational reliabilities and k-factors for converting reliability data from the storage environment to the operational environment. The storage reliability research program collected a

wide range of data from accelerated tests, special test programs, and a data bank on non-operating reliability developed for the U.S. Army Missile Command. Although classified as non-operational, the components are subjected to such relatively severe environments as transportation, handling, and test. The report covers electrical, electronic, electromagnetic, hydraulic, and pneumatic devices. Failure rates are grouped by part category and the best estimate is calculated along with 90 percent confidence intervals. In addition to failure rates, part failure modes are provided.

h) MIL-HANDBOOK 217. All electronic part failure rates were calculated using MIL-Handbook 217. The handbook methods were discussed in Section II and will be further elaborated on in this section.

i) Task I Data. Although the literature search provided much qualitative information, relatively little quantitative failure data was obtained. The quantitative data sources were discussed in Section IV.

B. DEVELOPMENT OF FAILURE RATES FOR COMMERCIAL VESSEL AUTOMATED CONTROLS

B.(1) Environmental K-Factors For Non-Electronic Parts.

As indicated in the above section, a great variety of data was available for this study. However, very little quantitative data specifically obtained from commercial vessel automation systems was found. In order to use data generated from other sources, such as for military applications and non-maritime environments, K-factors had to be developed. The purpose of these K-factors is for converting failure rates from other environments and other applications into ship system failure rates. It was also necessary to develop two sets of K-factors for the ship environment because of the radical difference between the controlled environment of the centralized engine control room and that of the "field" environment, (i.e., non-control room). The field environment is much more extreme in the areas of temperature, vibration, humidity, etc.

The closest environmental designation to commercial vessel application is that of "ship sheltered," as used in MIL-Handbook 217 and RADC documents. Therefore, ship sheltered (SHS) became the basis for all comparisons to other environments. Thus, with ship sheltered assigned a factor of 1, multipliers for other environments were then developed. All data sources were researched and where failure rates for ship sheltered and other environments were given for the same type parts, a ratio was

developed to convert to the ship sh .tered environment. Table VI-1 gives the individual part ty; s along with the environments and the environmental factors for each part type. As previously pointed out, the part types were grouped according to whether they were used in control room or field applications, and separate factors were developed for each. Because there was insufficient data and too much variability between breakdowns within part types, an average environmental factor (x) was developed for each environment (i.e. control room application and field application). In other words, to convert the failure rate for a switch or relay from a ground fixed (GRF) to a ship environment, the failure rate for the ground fixed environment is multiplied by 3.4633 to obtain a ship environment failure rate for a control room application. The field environment being much more severe, the conversion factor from a ground fixed to a ship field environment is 8.072. On the other hand, the aircraft uninhabited (AU) environment is much more severe than the ship environment, and converting failure rates from this environment to the ship environment requires that the aircraft environmental failure rate be multiplied by 0.1633. Environments listed in Table VI-I not mentioned above are ground mobile (GRM), airborne inhabited (AI), and submarine (SUB).

B.(2) Development Of Part Class And Type Failure Rates For Commerical Vessel Control Room Application

All applicable data sources were utilized to develop the failure rates for commercial vessel application. Table VI-2 summarizes the results of this data search.

B.(2)(a) Part Class and Type

Parts were grouped by class and type. In some cases, sufficient data was available to get individual failure rates by type; in other cases, the data was accumulated by class.

B.(2)(b) Sources

The sources are listed in Table VI-2 and have been described in some detail previously.

B.(2)(c) Environment

The environment from which the data source was obtained is given.

B.(2)(d) Application

The application of the part is either military (M) or commercial (C). In all cases, the mean calculation was used for generating the final failure information. However, as additional information, the lower confidence level, the upper confidence level, number of failures, and operating hours are given.

TABLE VI-1

K-Factor Development for Non-Electronic Parts
Factors for Converting Other Environments to Ship Sheltered

	GRF	GRM	AI	AU	SHS	SUB
CONTROL ROOM ENVIRONMENT						
CONNECTOR (217)	1.50	0.40	0.20	0.20	1.0	--
SWITCH (217)	1.33	0.23	0.40	0.04	1.0	--
RELAY-GENERAL (217)	3.75	1.00	0.94	0.25	1.0	--
RELAY-GENERAL	4.54	--	0.11	--	1.0	0.589
RELAY-ARMATURE	3.92	0.74	0.46	--	1.0	0.89
RELAY-	10.72	--	--	--	1.0	--
RELAY-TIME DELAY	1.11	0.37	0.09	--	1.0	2.37
SWITCH-PRESSURE	10.76	3.69	0.40	--	1.0	3.46
SWITCH-PUSHBUTTON	1.70	--	0.02	--	1.0	5.87
SWITCH-ROTARY	1.15	--	0.09	--	1.0	0.96
SWITCH-THERMOSTATIC	0.25	--	0.10	--	1.0	0.17
SWITCH-TOGGLE	0.83	0.17	0.07	--	1.0	--
$\bar{X}$	3.4633	0.9428	0.2618	0.1633	1.0	2.0441

	GRF	GRM	AI	AU	SHS	SUB
FIELD ENVIRONMENT						
ACTUATOR, LINEAR	0.74	0.21	0.06	0.15	1.0	7.04
SYNCHROS & RESOLVERS	3.01	--	0.63	--	1.0	36.77
FANS, AXIAL	5.89	1.14	0.05	--	1.0	--
PUMP	10.33	--	0.40	--	1.0	1.70
PUMP, CENTRIFUGAL	24.62	--	--	--	1.0	--
FAN, GENERAL	5.47	2.20	0.37	0.18	1.0	30.18
TURBINE/GENERATOR	0.02	1.20	--	--	1.0	--
GEAR	0.43	--	--	--	1.0	--
MECH. PWR. TRNSMSSN	1.05	0.15	--	0.16	1.0	--
MOTOR, GENERAL	8.29	--	--	--	1.0	4.55
PUMP, CENTRIFUGAL	24.81	--	--	--	1.0	--
PUMP, OIL	2.79	--	1.33	--	1.0	--
VALVE, GENERAL	24.83	--	5.67	0.01	1.0	--
TRANSFORMER (217)	4.0	2.0	0.19	0.14	1.0	--
SYNCHROS & RESOLVERS	4.8	0.73	1.47	0.35	1.0	--
$\bar{X}$	8.0720	1.0900	1.1300	0.1650	1.0	16.04

TABLE VI-2

Commercial Vessel Failure Rate Development for Non-Electronic Parts

Part Class and Type	Source	Env	App		Lower	Upper	Conf. Level	No. of Fails	Oper. Hours	Env. Adj. Factor	Part Type Basic SHS Failure Rate	Part Class Basic SHS Failure Rate	Percent Reduction due to Functional Test	Percent Reduction Inspt. and Sched. Maint.	Adjusted SHS Failure Rates for Test and Sched. Maint.
Valves, Without Operators															
(a1) Ball	SRI	NUC	C	2.838	--	2.25	Max	12	4.227	8.07	22.59				
(a2)	LMSC	--	C	4.6	0.4	7.07	99	--	--	--	--	--	--	--	--
(a3)	RAY	--	--	1.44	--	2.69	90	5	3.409	--	--	--	--	--	--
(b1) Butterfly	SRI	NUC	C	1.073	--	2.24	Max	7	6.521	8.07	8.66	--	--	--	--
(b2)	LMSC	--	M	3.4	1.3	5.3	99	--	--	--	--	--	--	--	--
(c) Globe	SRI	NUC	C	0.614	--	10.01	Max	4	6.515	8.07	4.95	12.07	30.0	39.3	3.70
Valves, Relief															
(a1)	RAY	GRM	M	2.517	2.1040	3.016	60	27	10.729	1.09	2.74	--	--	--	--
(a2)	LMSC	--	M	3.9	0.22	32.00	99	--	--	--	--	--	--	--	--
(a3)	RAY	GRF	--	1.51	--	2.100	90	17	11.23	8.07	12.19	--	--	--	--
(a4)	ARINC	SHS	M	0.90	--	--	--	2	0.220	1.00	0.90	5.27	30.0	39.3	1.62
Valves, Operators															
(a1) Pneumatic, Reverse Acting	SRI	NUC	C	3.426	--	24.03	Max	83	23.973	8.07	27.94	--	--	--	--
(a2) Pneumatic, Direct Acting	SRI	NUC	C	4.851	--	19.75	Max	134	27.626	8.07	39.15	--	--	--	--
(a3) Pneumatic, Double Acting	SRI	NUC	C	3.021	--	19.75	Max	35	11.587	8.07	24.38	30.49	28.1	30.2	
(b) Solenoid	SRI	NUC	C	4.760	--	29.77	Max	32	6.722	8.07	38.41	38.41	28.1	30.2	16.02

Table VI-2 (Cont.)

Commercial Vessel Failure Rate Development for Non-Electronic Parts

Part Class and Type	Source	Env	App		Lower	Upper	Conf. Level	No. of Fails	Oper. Hours	Env. Adj. Factor	Part Type Basic SHS Failure Rate	Part Class Basic SHS Failure Rate	Percent Reduction due to Functional Test	Percent Reduction Inspt. and Sched. Maint.	Adjusted SHS Failure Rates for Test and Sched. Maint.
(Transducers, continued)															
(d1) Resistance	SRI	NUC	C	0.938	--	4.73	Max	43	45.823	3.46	3.24	--	--	--	--
(d2) Thermo-couple	SRI	NUC	C	0.812	--	17.56	Max	35	43.101	3.46	2.81	--	--	--	--
(d3) Gen. Dyn. P/N2550799	GIDEP	NET	C	28.735	16.85	47.21	90	8	0.2784	1.00	28.74	--	--	--	--
(d4)	LMSC	--	M	3.3	1.5	6.4	99	--	--	--	--	--	--	--	--
(e) Flow	RAC	GRF	M	8.363	7.209	9.720	60	38	4.543	3.46	28.93	--	--	--	--
(f) Liquid Level															
(f1) Float	SRI	NUC	C	1.820	--	3.10	Max	12	6.591	3.46	6.30	--	--	--	--
(f2)	LMSC	--	M	2.6	0.35	3.7	--	--	--	--	--				
(g) Accelero-meter	RAC	GRM	M	35.078	33.38	36.88	60	303	8.638	1.09	37.14	20.95	28.4	27.6	9.22
Valves with Pneumatic Operators															
(a1) Pneumatic, General	RAY	GRF	--	6.640	--	8.900	90	21	3.164	8.07	53.58	--	--	--	--
(a2)	RAC	GRF	M	0.608	0.451	0.818	60	11	18.101	8.07	4.91	--	--	--	--
(a3) Pneumatic, Ball	SRI	NUC	C	2.496	--	2.685	Max	2	0.801	8.04	20.14	--	--	--	--
(a4) Pneumatic, Butterfly	SRI	NUC	C	1.675	--	17.56	Max	14	8.658	8.01	13.52	--	--	--	--
(a5) Pneumatic, Check	SRI	NUC	C	4.935	--	17.57	Max	5	1.013	8.07	39.83	--	--	--	--
(a6) Pneumatic, Gate	SRI	NUC	C	2.637	--	13.17	Max	9	3.412	8.07	18.86	--	--	--	--
(a7) Pneumatic, Globe	SRI	NUC	C	9.715	--	76.07	Max	68	6.999	8.07	78.40	32.75	26.0	28.0	15.06
Valves, Hydraulic															
(a) General	RAC	GRM	M	7.302	6.320	8.452	60	40	5.478	1.09	7.96	--	--	--	--
(b1) Check	SRI	NUC	C	0.850	--	5.00	Max	9	10.582	8.07	6.86	--	--	--	--
(b2)	RAC	GRF	M	3.180	2.735	3.704	60	37	11.636	8.07	25.66	--	--	--	--
(b3)	LMSC	--	M	2.3	0.11	4.7	99	--	--	--	--	--	--	--	--
(c) Servo	LMSC	--	M	30.0	16.0	56.0	99	--	--	--	--	--	--	--	--
	SRI	NUC	C	4.20	--	144.16	Max	22	5.238	8.07	33.89	18.59	26.0	28.0	8.55

Table VI-2 (Cont.)

Commercial Vessel Failure Rate Development for Non-Electronic Parts

Part Class and Type	Source	Env	App		Lower	Upper	Conf. Level	No. of Fails	Oper. Hours	Env. Adj. Factor	Part Type Basic SHS Failure Rate	Part Class Basic SHS Failure Rate	Percent Reduction due to Functional Test	Percent Reduction Inspt. and Sched. Maint.	Adjusted SHS Failure Rates for Test and Sched. Maint.
Pumps															
(a) Hydraulic	RAC	GRM	M	42.637	41.241	43.675	60	897	21.137	1.09	46.26	--	--	--	--
	RAY	GRM	--	67.00	--	69.300	90	1,442	21.514	1.09	73.03	59.64	49.3	3.1	28.39
Regulators															
(a) Pressure	RAC	GRF	M	2.435	2.145	2.768	60	51	20.946	8.07	19.65	19.65	--	--	--
Relays															
(a1) General	RAC	SHS	C	0.9732	0.825	1.054	60	55	59.003	1.00	0.93	--	--	--	--
(a2) General	217	SHS	C	0.78	--	--	--	--	--	--	0.78	--	--	--	--
(a3) General	RAY	SHS	--	0.754	--	1.048	90	17	22.55	1.00	0.75	--	--	--	--
(b) Armature	RAY	SHS	--	0.915	--	1.034	90	116	126.7	1.00	0.91	--	--	--	--
(c) Reed	RAY	SHS	--	1.973	--	2.443	90	39	19.77	1.00	1.97	1.06	46.0	27.6	0.32
Electro-Mechanical															
(a) Blower/Fan	RAC	SHS	M	13.761	12.659	14.973	60	112	8.138	1.0	13.76	--	--	--	--
(b) Solenoids	RAC	AIT	C	18.031	13.761	23.646	60	13	0.721	0.26	4.68	--	--	--	--
	GIDEP	SUB	M	22.755	11.181	44.056	60	4	0.175	2.04	46.43	21.62	18.9	63.2	3.87
Switches															
(a1) General	RAC	GRF	M	1.986	1.633	2.420	60	23	11.581	3.46	6.87	--	--	--	--
(a2)	217	SHS	C	0.17	--	--	--	--	--	1.00	0.17	--	--	--	--
(b) Flow	GIDEP	SUB	M	2.428	1.380	4.105	90	7	2.883	2.04	4.95	--	--	--	--
(c) Pressure	RAC	SHS	M	22.556	18.021	28.286	60	18	0.798	1.00	22.56	--	--	--	--
(d) Pushbutton	RAY	SHS	--	0.458	--	0.548	90	55	120.2	1.00	0.46	--	--	--	--
(e) Toggle	RAY	SHS	--	0.478	--	0.557	90	67	141.2	1.00	0.48	--	--	--	--
(f) Liquid Level	RAC	GRF	M	5.277	3.029	8.839	60	4	0.758	3.46	18.26	--	--	--	--
(g) Limit-Micro	SRI	NUC	C	0.839	--	20.48	Max	70	83.683	3.46	2.90	7.08	28.4	27.6	3.11
Transducers															
(a) General	RAC	AI	C	91.917	87.067	97.082	60	257	2.796	0.26	23.90	--	--	--	--
(b) General	RAC	GRF	M	2.980	2.546	3.496	60	34	11.409	3.46	10.31	--	--	--	--
(c) Pressure	RAC	AUT	C	54.106	51.61	56.34	60	33.6	6.210	0.16	8.66	--	--	--	--
(c1) Diaphram	SRI	NUC	C	2.024	--	6.69	Max	56	27.659	3.46	7.00	--	--	--	--
(c2) Rosemount PN1201FA4A 1B	GIDEP	WET	C	18.3382	--	--	--	3	0.163	1.00	18.38	--	--	--	--
(c3)	LMSC	--	M	3.5	1.7	6.6	99	--	--	--	--	--	--	--	--
(d) Temp.	RAC	GRF	C	21.964	18.758	25.768	60	34	1.548	3.46	75.98	--	--	--	--

Table VI-2 (Cont.)

Commercial Vessel Failure Rate Development for Non-Electronic Parts

Part Class and Type	Source	Env	App		Lower	Upper	Conf. Level	No. of Fails	Oper. Hours	Env. Adj. Factor	Part Type Basic SHS Failure Rate	Part Class Basic SHS Failure Rate	Percent Reduction due to Functional Test	Percent Reduction Inspt. and Sched. Maint.	Adjusted SHS Failure Rates for Test and Sched. Maint.
Actuators															
(a) General	RAC	AUT	C	101.429	98.806	104.134	60	1,065	10.500	0.17	17.24	--	--	--	--
(a2) General	LMSC	--	M	5.1	0.10	36.0	99	--	--	--		--	--	--	--
(b) Hydraulics	RAC	GRF	M	0.290	0.057	0.880	60	1	3.454	8.37	2.34	--	--	--	--
	GIDEP	AIF	M	0.345	--	--	--	58	197.202	1.13	0.40	--	--	--	--
(c) Linear	RAC	SHS	M	1.707	6.622	17.014	60	5	0.467	1.0	10.71	7.67	--	--	--
Connectors															
(a) Circular	RAC	SHS	M	0.071	0.055	0.092	60	14	197.465	1.0	0.07	--	--	--	--
(b) Coaxial	RAC	SHS	M	0.017	0.003	0.053	60	1	57.253	1.0	0.02	0.05	28.4	27.6	6.02
Controls and Instruments															
(a) Controller Pneumatic-Proportional	SRI	MUC	C	0.114	--	1.76	Max	1	8.07	0.92	--	--	--	--	--
(b) Controller Pneumatic On-Off	SRI	MUC	C	0.608	--	3.19	Max	4	6.574	8.07	4.91	2.92	28.4	27.6	1.28
(c) Pneumatic Control Modules															
(d) Electronic Control Modules															
Controls and Instruments															
(a) Indicator	RAC	GRM	C	70.413	64.696	76.709	60	109	1.548	1.09	76.75	--	--	--	--
Power Supplies															
(a) 1-30 Volts	GIDEP	BUB	M	5.077	2.495	2.495	90	---	---	2.04	10.36	--	--	---	--
(b)	EERD	AI	M	8.319	--	--	--	--	--	0.26	2.36	--	--	--	--
(c)	EERD	AI	M	85.903	--	--	--	--	--	0.26	22.33	--	--	--	--
(d)	EERD	AI	M	7.700	--	--	--	--	--	0.26	2.00	9.26	28.4	27.6	4.07

B.(2)(e) Environmental Adjustment Factor

The environmental adjustment factor, as explained above, is entered for part classes and types.

B.(2)(f) Part Type, Basic Ship Sheltered Failure Rate

This is the product of the mean failure rate for the specific environment times the adjustment factor to convert the failure rate to a ship sheltered environment.

B.(2)(g) Part Class, Basic Ship Sheltered Failure Rate

Part class, basic ship sheltered failure rate is the average of the class.

B.(2)(h) Percent Reduction due to Functional Test

For each class, a percent reduction that can be obtained due to functional test is provided.

B.(2)(i) Percent Reduction due to Inspection and Scheduled Maintenance

The percentage obtained for reducing the failure rate due to inspection and scheduled maintenance is given.

B.(2)(j) Adjusted Ship Sheltered Failure Rates for Test and Scheduled Maintenance

This is the basic failure rate less the percentages that can be eliminated due to functional tests, inspection and scheduled maintenance. These are the most optimistic failure rates.

B.(3) Adjustment Factors For Reducing Basic Failure Rates Through Functional Testing, Inspection, And Scheduled Maintenance

In order to develop the relative failure rate improvements obtainable through functional testing, operational testing, inspection, and preventative maintenance, certain assumptions had to be made. These assumptions are as follows.

a) The failure rates derived from historical data and adjusted by the K-factors are basic failure rates. These basic failure rates are the so-called "unscheduled maintenance action" failure rates. That is, they apply to hardware problems requiring unscheduled maintenance. All unscheduled maintenance actions are not always the result of operational failures. However, if the unscheduled maintenance is not performed, it can be reasonably assumed that the defect will eventually degrade to the point where it becomes a functional failure.

b) It is assumed that certain failures can be detected prior to functional failure, either through functional testing or inspection, or that they can be prevented through preventative maintenance.

c) Other failures occur instantaneously and cannot be detected prior to failure and therefore, cannot be prevented.

Another class of failure is the wear-out type which can be prevented by scheduled removals. All these types of failures are included in the basic failure rates.

Based on historical data, the percentage of failures by part class that can be eliminated through functional testing and through maintenance was determined. Maintenance includes scheduled inspection and scheduled preventative maintenance. These percentages were derived from historical data that broke out how the failures were detected. In other words, for certain part types, the data gives the percentage of failures that were detected during functional test, during inspection, and during other categories of activities. Much of this data was obtained from the nuclear failure rate information generated by the Southwest Research Institute. This data was very precise, and in many cases, the total operating hours were in excess of many millions of hours.

B.(4) Adjustment Factors For "Opens" From The Field

Both historical data and the open literature indicate that a major problem with control systems concerns the workmanship of the interconnections from the field components to the control console. That is, these interconnections are prone to "fail open". Various documents indicate that the magnitude of this problem is directly related to the shipyard performing the work. However, after a period of time, which can vary from six months to approximately three years, these problems are eventually eliminated and a steady state condition as far as "opens" from the field is reached.

In order to adjust the data for potential field opens, DOVAP added 0.38 failures per million hours for each field connection. This breaks down as follows:

a) 0.33 failures per million hours for cable to console failure rates

b) 0.04 failures per million hours for connector failure rates

c) 0.01 failures per million hours for connection of the cable to the field component.

B.(5) Substantiation Of Six Month Factors For Hardware Other Than Electronic Components.

The average decrease in failure rates from the infant mortality period to the steady state period was obtained from the report "Consideration for the Initial Failures of Marine Engines," Log Number 075. This report shows a considerable difference in failure frequencies between the first six month period and the remaining period over which data was collected.

From the data in the report, the total number of failures for the first six month period and for all failures occurring after six months can be obtained. This amounts to 11.72 failures per ship month for the first six months, and 2.98 failures per ship month after the initial first six months. This report also subdivides data by equipment classification such as automation equipment, and piping and valves. From this, the percent contribution of valves and piping and of automation systems were broken out from the total. This amounted to 7.4 per month for valves and piping for the initial period, and .64 for the period past six months. For the automation systems, it amounted to 3.3 failures for the first six months and then the failure rate leveled out to .5 per month after the initial six month period. Using these ratios, automation failures, excluding electronics, for the first six months are 6.6 times higher than that of the steady state period. For valves, piping,and other field components, it was estimated that the premature failure rate is 11.6 times higher than that of the steady state condition.

C. ELECTRONIC PARTS STRESS ANALYSIS

As can be recalled from Section II, "Fundamentals of Reliability", MIL-Handbook 217 utilizes part stress ratios as factors in the failure rate equation. These part stress factors are the ratio of the actual value to the rated value for the appropriate part parameters. (For instance, for transistors, power is one of the parameters.)

In order to develop these stress factors so that failure rates could be obtained from MIL-Handbook 217, circuit analyses were performed. These analyses were conducted on a sample of the electronic components in the control systems of all 3 vessels. The sample represents about 20 percent of the printed circuit card types; however, these are the high usage cards and represent approximately 70 percent of the total electronic parts used in the systems.

In conducting the parts stress analysis, power dissipation, current, and voltage stress values were computed based on

nominal supply voltages. Component ratings, as shown on the schematic, were taken as the base level component rating, e.g., if a resistor was listed as 1/4 watt, stress levels were computed considering 1/4 watt as 100 percent.

Stress factors for Systems B and C circuitry which drove off-card circuits were computed by using maximum operating conditions as described in the module specification. There were some cases where this information was not available, however, most of the card output circuits were loaded similarly to those in the documented circuits.

System A circuit cards used logic devices and op-amps driving off-card loads. Stress factors for digital IC's were computed assuming a worst case device power supply current and multiplying it by the nominal power supply voltage. Analog devices were assumed to be driving their maximum guaranteed load current into a resistive ground-referred load. For signal amplifiers, the output load current was computed using the worst case power dissipation condition in the device output region of +10 volts.

In conducting the part stress analysis, worksheets were used to record the values computed. Figure VI-1 depicts a sample of these worksheets.

D. RELIABILITY GROWTH AND THE EFFECT OF SCREENED AND UNSCREENED CIRCUIT CARDS

A great deal of data has been generated on the subject of reliability growth of electronic components and on the effects of environmental screening or burn-in. One such paper is "The Reliability Growth, Screened vs. Nonscreened Computers"*. This paper documents the reliability improvement factor identified when digital computer circuit cards were subjected to a set of environmental screens, as compared to identical cards without environmental screening. Rates of reliability growth were identified for each type of card. All components used were of Mil-grade quality and were derated according to applicable NASA requirements.

The burned-in components were subjected to 200 hours in a chamber which cycled the temperature of the units from a -40° F to $+105^{\circ}$ F. The rate of reliability growth for the two types of printed circuit assemblies is shown in Figure VI-2. The following was concluded from the data.

*1982 Proceedings, Annual Reliability and Maintainability Symposium, E.W. Derenthal, IBM Corporation, Oswego, N.Y.

Assy

FIGURE VI-1
Example of Component Stress Ratio
and Temperature Rise Worksheet

Type	Number of Entries	I. D. Number	Rating - Value	Stress Ratio	Temperature Rise °C	
LM308L	6	U2, U4, U6, U8 U10, U12			6°	7 pins active TO-5 6 pins active
LM741L	1	U13			10°	TO5 5 pins active
LM342	6	U1, U2, U5, U7, U9, U11			11°	14 PINS active 20 Ω DIP-14
JAN 1N829	1	CR1		.12	15°	6.2 V ... TO-46
CL	15	C1, C2, C21-C33	68uF 100V	.43		
CK	12	C3-C7, C9, C10 C12, C13, C15 C18, C19	.01uF 200V	.075		
↓	6	C8, C11, C14, C16 C17, C20	330pF 1KV	.01		
2N2219A	6	Q1-Q6		.47	42°	192 mW
Potentiometer CT	6	R114, R117, R120 R123, R126 R129	5K	.01		.75 W cermet
↓	13	R113, R115, R116 R118, R119, R121 R122, R124, R125	10K	.01		.75 W cermet
		R127, R128, R130 R131				
RN55	1	R111	1.15K	.54		
↓	1	R102	61.9K	.01		
↓	1	R110	28K	.01		
↓	13	Find # 15	45.3K	.01		
↓	24	Find # 16	100K	.01		

The reliability improvement factor for screened units over nonscreened units is not consistent but rather a function of age. The factor observed for the screened unit was 2.5 at 1,000 hours, 1.6 at 5,000 hours, and approached unity at 30,000 hours. The screened units start at an initially higher mean time between failure than the unscreened units, but demonstrate a lower reliability growth rate. The curves show that generally higher reliability can be obtained by units that have been subjected to burn-in or thermal cycling. Both screened and unscreened units will demonstrate reliability growth; however at approximately 30,000 hours the rate of growth becomes approximately the same.

No data could be found showing the rate of growth for commercial grade components. Therefore, the growth rate selected for the commerical vessels on this study was the unscreened rate for the Mil-grade parts as shown in Figure VI-2. It is assumed that initial failure rates are higher and the rate of growth is substantially higher for commercial grade components because the individual components had not been screened or burned in.

Because of the significant initial improvement in burned-in assemblies, it is recommended that manufacturers of propulsion control systems burn-in and thermal cycle the printed circuit cards.

E. ELECTRONIC PART FAILURE RATE GENERATION

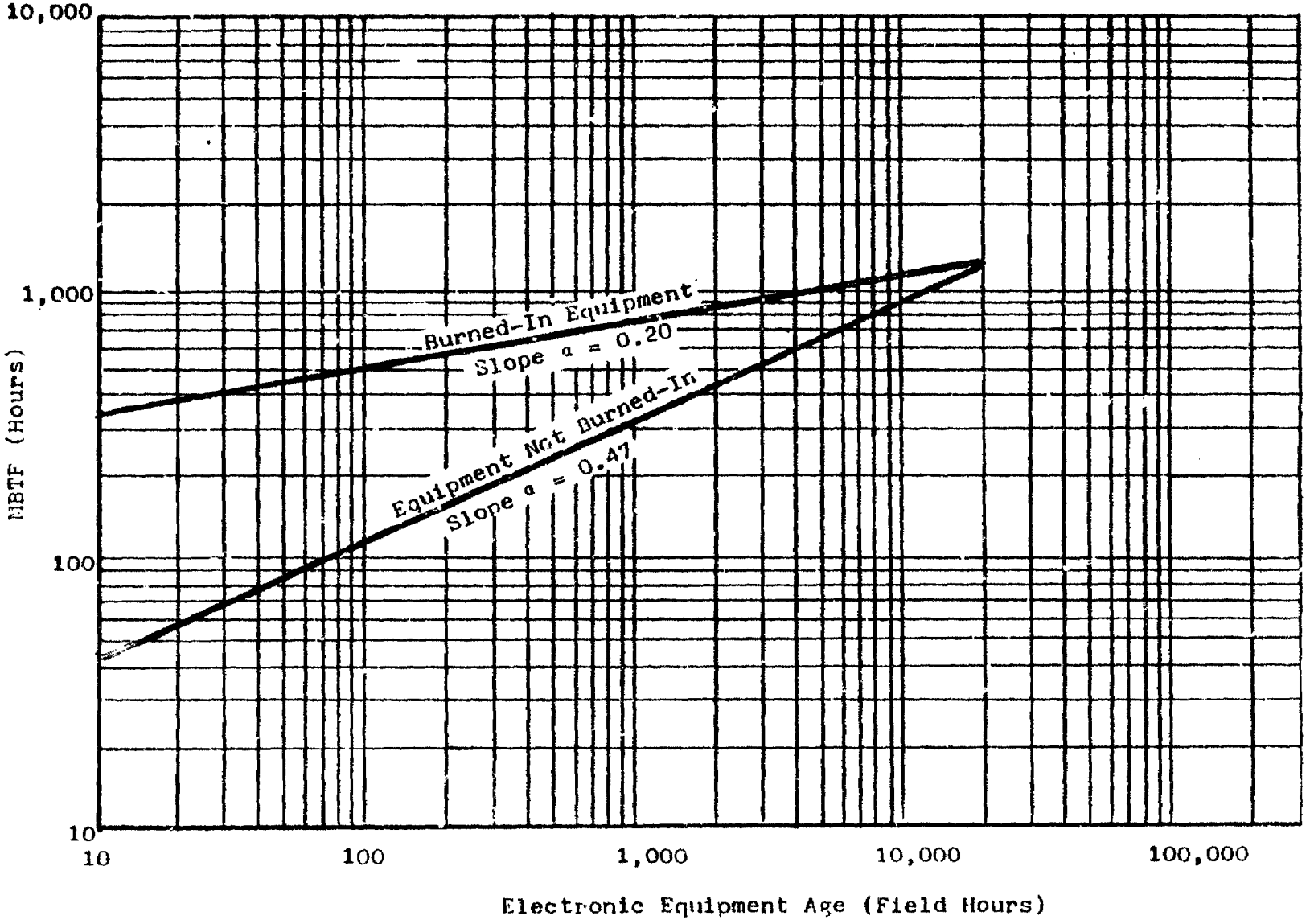
E.(1) Application Of MIL-Handbook 217.

The electronic part failure rates used by DOVAP were obtained from MIL-Handbook 217. In order to facilitate development of these failure rates, computer software was utilized. This computer software is called PREDICTOR and was developed by Management Sciences, Inc. of Albuquerque, New Mexico. To generate failure rates using PREDICTOR, the user supplies the program with data elements such as component types, quantities, quality levels, stresses, ambient temperature, environments, etc.. The program recognizes key words and data that are relevant to the failure rate predictions. Examples of key words are component nomenclature and component part type designation numbers. Through built-in program defaults, predictions will be developed utilizing whatever data the software has available.

Figure VI-3 shows the PREDICTOR output for a sample of 121 electronic parts. The basic methods for developing failure rates from MIL-Handbook 217 were described in Section II, and as explained in that section, many factors are used in the failure

Figure VI-2

Reliability Growth of Electronic Equipment



LEVEL 3

	STRESS RATIO (S)	ITEM FAILURE RATE	MIL SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	DT C.	RL	SR2	RATED/ RATING T/BITS	STYLE/ MODEL	RT
RESISTOR ST=RN	0.20	0.00470	0.00940	5	0.04702	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.00157	0.00470	4	0.01881	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RW	0.20	0.03382	0.06764	1	0.06764	0.0	MIL	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.00157	0.00470	1	0.00470	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00172	0.00517	1	0.00517	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00157	0.00470	2	0.00941	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.00517	0.01034	1	0.01034	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.03382	0.06764	2	0.13527	0.0	MIL	0.0	125.	RW	40
RESISTOR ST=RW	0.20	0.03382	0.06764	7	0.47346	0.0	MIL	0.0	125.	RW	40
RESISTOR ST=RN	0.20	0.00470	0.00940	1	0.00940	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RN	0.20	0.00470	0.00940	1	0.00940	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.00470	0.00940	1	0.00940	0.0	MIL	0.0	125.	RW	43
RESISTOR ST=RC	0.20	0.00157	0.00470	1	0.00470	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.00470	0.00940	1	0.00940	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.00172	0.00517	1	0.00517	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00157	0.00470	1	0.00470	0.0	MIL	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.00470	0.00940	2	0.01881	0.0	MIL	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.03382	0.06764	1	0.06764	0.0	MIL	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.00172	0.00517	1	0.00517	0.0	MIL	0.0	125.	RC	38
CAPACITOR ST=CK	0.20	0.00222	0.00554	1	0.00554	0.0	MIL	0.0	125.	CK	22
CAPACITOR ST=CB	0.20	0.00035	0.00087	1	0.00087	0.0	MIL	0.0	85.	CB	32
CAPACITOR ST=CL	0.20	0.00967	0.05801	1	0.05801	0.0	MIL	0.0	125.	CL	14
CAPACITOR ST=CK	0.20	0.00155	0.00388	2	0.00776	0.0	MIL	0.0	125.	CK	22
CAPACITOR ST=CB	0.20	0.00042	0.00105	1	0.00105	0.0	MIL	0.0	85.	CB	32
CAPACITOR ST=CL	0.20	0.01016	0.06098	2	0.12195	0.0	MIL	0.0	125.	CL	14
CAPACITOR ST=CB	0.20	0.00016	0.00040	1	0.00040	0.0	MIL	0.0	85.	CB	32
DIODE 1N5230B QUAL	0.20	0.00170	0.01703	1	0.01703	0.0	J	0.20	175.	L	58
DIODE 1N457 QUAL	0.20	0.00170	0.01703	1	0.01703	0.0	J	0.20	175.	L	54
LINEAR IC		0.11439	0.29032	1	0.29032	10.0	B2	0.0	22.		98
DIGITAL IC		0.03702	0.13849	1	0.13849	10.0	B2	0.0	4.		99
TRANSISTOR 2N2643 QUAL	0.20	0.00329	0.03290	1	0.03290	0.0	J	0.20	175.	2N2643	61
TRANSISTOR 2N1893 QUAL	0.20	0.00329	0.03290	1	0.03290	0.0	J	0.20	175.	2N1893	61
CAPACITOR ST=CK	0.20	0.00512	0.01279	1	0.01279	0.0	MIL	0.0	125.	CK	22
TOTAL				91							
TOTAL FAILURE RATE (35.0 C)					1.65266						
MTBF(HOURS) (69.15 YRS.)					605085.312						

FIGURE VI-3
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C, and lower military grade quality.)

LEVEL 2

	STRESS RATIO (S)	ITEM FAILURE RATE	NO SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	QT C.	RL	SR2	GATES/ RATING T/BITS	STYLE/ MODEL	RT
DIODE 1N5305 QUAL	0.20	0.00170	0.01703	1	0.01703	0.0	J	0.20	175.	L	54
RESISTOR STANRN	0.20	0.00626	0.01251	1	0.01251	30.0	MS	0.0	125.	RN	43
RESISTOR STANRC	0.20	0.01161	0.03484	3	0.03484	30.0	MS	0.0	125.	RC	38
RESISTOR STANRW	0.20	0.04396	0.08791	1	0.08791	30.0	MS	0.0	125.	RW	40
RESISTOR STANRC	0.20	0.00464	0.01393	1	0.01393	30.0	MS	0.0	125.	RC	38
RESISTOR STANRN	0.20	0.00626	0.01251	2	0.02503	30.0	MS	0.0	125.	RN	43
RESISTOR STANRW	0.20	0.04396	0.08791	1	0.08791	30.0	MS	0.0	125.	RW	40
RESISTOR STANRC	0.20	0.00511	0.01533	1	0.01533	30.0	MS	0.0	125.	RC	38
CAPACITOR STANCB	0.20	0.00078	0.00194	2	0.00388	30.0	MS	0.0	85.	CB	32
CAPACITOR STANCK	0.20	0.00239	0.00598	3	0.01793	30.0	MS	0.0	125.	CK	22
CAPACITOR STANCL	0.20	0.01356	0.08139	1	0.08139	30.0	MS	0.0	125.	CL	14
TRANSISTOR NPN QUAL	0.20	0.00329	0.03290	1	0.03290	0.0	J	0.20	175.	NPN	61
LINEAR IC QUAD-1		0.11439	0.29032	1	0.29032	10.0	B2	0.0	22.	D-1	98
CAPACITOR STANCB	0.20	0.00028	0.00070	1	0.00070	30.0	MS	0.0	85.	CB	32
RESISTOR STANRN	0.20	0.00626	0.01251	1	0.01251	30.0	MS	0.0	125.	RN	43
CAPACITOR STANCK	0.20	0.00135	0.00338	1	0.00338	30.0	MS	0.0	125.	CK	22
DIODE 1N2071 QUAL	0.20	0.00170	0.01703	1	0.01703	0.0	J	0.20	175.	L	54
TOTAL				21							

TOTAL FAILURE RATE (35.0 C) 0.75455

MTBF(HOURS) 1325301.00
(151.46 YRS.)

FIGURE VI-3 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C, and lower military grade quality.)

LEVEL 1

	STRESS RATIO (S)	ITEM FAILURE RATE	MB SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	DT C.	RL	SR2	GATES/ RATING T/BITS	STYLE/ MODEL	RT
DIGITAL IC		0.03782	0.13849	1	0.13849	10.0	B2	0.0	4.		99
DIGITAL IC		0.03837	0.14096	1	0.14096	10.0	B2	0.0	4.		99
DIGITAL IC		0.03782	0.13849	1	0.13849	10.0	B2	0.0	4.		99
DIODE 1N457	0.20	0.00176	0.01703	14	0.23846	0.0	J	0.20	175.	1N457	58
TRANSISTOR 2N4250	0.20	0.00492	0.04924	2	0.09849	0.0	J	0.20	175.	2N4250	60
TRANSISTOR 2N3566	0.20	0.00329	0.03290	1	0.03290	0.0	J	0.20	175.	2N3566	61
TRANSISTOR 2N6028	0.20	0.00205	0.02450	2	1.64900	0.0	J	0.20	175.	2N6028	96
CAPACITOR ST=CK	0.20	0.00125	0.00313	3	0.00940	0.0	MB	0.0	125.	CK	22
CAPACITOR ST=CS	0.20	0.00044	0.00110	1	0.00110	0.0	MB	0.0	85.	CS	32
CAPACITOR ST=CL	0.20	0.01016	0.06098	3	0.18293	0.0	MB	0.0	125.	CL	14
CAPACITOR ST=CS	0.20	0.00042	0.00104	1	0.00104	0.0	MB	0.0	85.	CS	32
CAPACITOR ST=CS	0.20	0.00024	0.00060	1	0.00060	0.0	MB	0.0	85.	CS	32
CAPACITOR ST=CL	0.20	0.00873	0.05238	1	0.05238	0.0	MB	0.0	125.	CL	14
RESISTOR ST=RN	0.20	0.00474	0.00948	1	0.00948	0.0	MB	0.0	125.	RN	43
RESISTOR ST=RM	0.20	0.03382	0.06764	2	0.13527	0.0	MB	0.0	125.	RM	48
RESISTOR ST=RC	0.20	0.00157	0.00470	2	0.00941	0.0	MB	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.00517	0.01034	3	0.03103	0.0	MB	0.0	125.	RN	41
RESISTOR ST=RM	0.20	0.03382	0.06764	3	0.20291	0.0	MB	0.0	125.	RM	48
RESISTOR ST=RN	0.20	0.00470	0.00940	1	0.00940	0.0	MB	0.0	125.	RN	43
RESISTOR ST=RM	0.20	0.03382	0.06764	1	0.06764	0.0	MB	0.0	125.	RM	48
RESISTOR ST=RN	0.20	0.00470	0.00940	1	0.00940	0.0	MB	0.0	125.	RN	43
RESISTOR ST=RM	0.20	0.03382	0.06764	1	0.06764	0.0	MB	0.0	125.	RM	48
TRANSISTOR 2N4250 QUAL	0.20	0.00492	0.04924	1	0.04924	0.0	J	0.20	175.	2N4250	60
RESISTOR ST=RC	0.20	0.00157	0.00470	1	0.00470	0.0	MB	0.0	125.	RC	38
TOTAL				49							

TOTAL FAILURE RATE (35.0 C) 3.28027

MTBF(HOURS) 304852.750
(34.84 YRS.)

FIGURE VI-3 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C, and lower military grade quality.)

rate equations. Some of these factors have minor effects on the final rate value. Some are significant however, and those which DOVAP used in the calculations are described as follows:

Ambient Temperature; An ambient temperature of 35° C. was used for the electronic part failure rate calculations. The 35° C. was estimated as the upper range of the actual operating temperatures within the control consoles. Where certain components run hotter at the junction than the estimated ambient, a junction temperature rise was also added to the ambient for those components. The actual range observed aboard one ship was 72° to 75° F. and this remained fairly constant. The control cabinets usually contained blowers which circulate the air, and the ambient should be fairly well distributed within the cabinet.

Quality Level; The commercial quality level was used for all component failure rate predictions. The quality level factor can have a very significant effect upon the end failure rate.

Operating Stress Ratio; As previously described, stress analysis was performed on approximately 70 percent of the electronic parts covered in this study. The remaining stress ratios were estimated based upon these calculated values.

Environment; The naval sheltered environment was used for this analysis. The MIL-Handbook 217 decription for this environment covers components located below deck and protected from weather, and includes such equipment as ship communications, computers, and sonar equipment.

E.(2) Analysis Of The Effect of Temperature

Because of the possibility that some control rooms are not air conditioned, the effects of higher temperature levels were evaluated. This was accomplished by generating failure rate predictions for a sample of 121 electronic parts at temperatures of both 35° C. and 50° C.. These data printouts are provided in Figures VI-4 and VI-5. The total failure rate for the 121 parts at 35 C. was 24.8343 failures per million hours. The failure rate increased to 32.899 failures per million hours for the 50° C. condition, for an overall failure rate increase of approximately 32 percent. However, the majority of the increase is due to semiconductors and ICs which become more failure prone as the temperature increases.

LEVEL 1

	STRESS RATIO (S)	ITEM FAILURE RATE	NS SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	PT C.	RL	SR2	GATES/ RATING T/BITS	STYLE/ MODEL	RT
DIGITAL IC		0.21200	0.70954	1	0.70954	10.0	DI	0.0	4.		99
DIGITAL IC		0.21993	0.00353	1	0.00353	10.0	DI	0.0	4.		99
DIGITAL IC		0.21200	0.70954	1	0.70954	10.0	DI	0.0	4.		99
DIODE 1N457	0.20	0.00052	0.00516	14	1.19230	0.0	L	0.20	175.	1N457	54
TRANSISTOR 2N4250	0.20	0.02462	0.24622	2	0.49244	0.0	L	0.20	175.	2N4250	60
TRANSISTOR 2N3546	0.20	0.01645	0.16449	1	0.16449	0.0	L	0.20	175.	2N3546	61
TRANSISTOR 2N6028	0.20	0.41	0.12250	2	0.24500	0.0	L	0.20	175.	2N6028	96
CAPACITOR ST=CK	0.20	0.00019	0.01045	3	0.03134	0.0	LW	0.0	125.	CK	22
CAPACITOR ST=C8	0.20	0.00441	0.01103	1	0.01103	0.0	LW	0.0	85.	C8	32
CAPACITOR ST=CL	0.20	0.01016	0.06098	3	0.18293	0.0	MB	0.0	125.	CL	14
CAPACITOR ST=C8	0.20	0.00415	0.01039	1	0.01039	0.0	LW	0.0	85.	C8	32
CAPACITOR ST=C8	0.20	0.00242	0.00605	1	0.00605	0.0	LW	0.0	85.	C8	32
CAPACITOR ST=CL	0.20	0.03918	0.17459	1	0.17459	0.0	LW	0.0	125.	CL	14
RESISTOR ST=RN	0.20	0.01410	0.02821	1	0.02821	0.0	LW	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.10145	0.20291	2	0.40582	0.0	LW	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.00470	0.01411	2	0.02822	0.0	LW	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.01552	0.03103	3	0.09309	0.0	LW	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.10145	0.20291	3	0.60873	0.0	LW	0.0	125.	RW	40
RESISTOR ST=RN	0.20	0.01410	0.02821	1	0.02821	0.0	LW	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.10145	0.20291	1	0.20291	0.0	LW	0.0	125.	RW	40
RESISTOR ST=RN	0.20	0.01410	0.02821	1	0.02821	0.0	LW	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.10145	0.20291	1	0.20291	0.0	LW	0.0	125.	RW	40
TRANSISTOR 2N4250 QU=L	0.20	0.02462	0.24622	1	0.24622	0.0	L	0.20	175.	L	60
RESISTOR ST=RC	0.20	0.00470	0.01411	1	0.01411	0.0	LW	0.0	125.	RC	38
TOTAL				49							

TOTAL FAILURE RATE 14.77979
(35.0 C)

MTBF(HOURS) 67659.9375
(7.73 YRS.)

FIGURE VI-4
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C, and commercial grade quality.)

LEVEL 2

	STRESS RATIO (S)	ITEM FAILURE RATE	NS SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	BT C.	RL	πR2	GATES/ RATING W/BITS	STYLE/ MODEL	RT
DIODE IN5305 DUAL	0.20	0.00852	0.00516	1	0.00516	0.0	L	0.20	175.	L	54
RESISTOR ST=RN	0.20	0.01877	0.03754	1	0.03754	30.0	LW	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.05404	0.10451	1	0.10451	30.0	LW	0.0	125.	RC	3A
RESISTOR ST=RW	0.20	0.13187	0.26374	1	0.26374	30.0	LW	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.01303	0.04180	1	0.04180	30.0	LW	0.0	125.	RC	3A
RESISTOR ST=RN	0.20	0.01877	0.03754	2	0.07508	30.0	LW	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.13187	0.26374	1	0.26374	30.0	LW	0.0	125.	RW	40
CAPACITOR ST=CB	0.20	0.01553	0.00598	1	0.00598	30.0	LW	0.0	125.	RC	38
CAPACITOR ST=CK	0.20	0.00777	0.01942	2	0.03883	30.0	LW	0.0	85.	CB	32
CAPACITOR ST=CL	0.20	0.00797	0.01992	3	0.05977	30.0	LW	0.0	125.	CK	22
TRANSISTOR NPN DUAL	0.20	0.04522	0.27130	1	0.27130	30.0	LW	0.0	125.	CL	14
LINEAR IC DUAD-1	0.20	0.01685	0.16849	1	0.16849	0.0	L	0.20	175.	NPN	61
CAPACITOR ST=CB		0.87945	1.85792	1	1.85792	10.0	DI	0.0	22.	D-1	94
RESISTOR ST=RN	0.20	0.00282	0.00704	1	0.00704	30.0	LW	0.0	85.	CB	32
CAPACITOR ST=CK	0.20	0.01877	0.03758	1	0.03758	30.0	LW	0.0	125.	RN	43
DIODE IN2071 DUAL	0.20	0.00451	0.01126	1	0.01126	30.0	LW	0.0	125.	CK	22
	0.20	0.00852	0.00516	1	0.00516	0.0	L	0.20	175.	L	54
TOTAL				21							

TOTAL FAILURE RATE
(35.0 C) 3.45088

MTBF(HOURS) 289781.125
(33.12 YRS.)

FIGURE VI-4 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C and commercial grade quality.)

LEVEL 3

	STRESS RATIO (S)	ITEM FAILURE RATE	MB SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	DT C.	RL	BR2	CATEG/ RATING T/BITS	STYLE/ MODEL	RT
RESISTOR ST=RN	0.20	0.01410	0.02021	5	0.10105	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.00470	0.01411	4	0.05644	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.10145	0.20291	1	0.20291	0.0	LN	0.0	125.	RN	40
RESISTOR ST=RC	0.20	0.00470	0.01411	1	0.01411	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00517	0.01552	1	0.01552	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00470	0.01411	2	0.02822	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.01552	0.03103	1	0.03103	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RN	0.20	0.10145	0.20291	2	0.40582	0.0	LN	0.0	125.	RN	40
RESISTOR ST=RN	0.20	0.10145	0.20291	7	1.42037	0.0	LN	0.0	125.	RN	40
RESISTOR ST=RN	0.20	0.01410	0.02021	1	0.02021	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RN	0.20	0.01410	0.02021	1	0.02021	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RN	0.20	0.01410	0.02021	1	0.02021	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.00470	0.01411	1	0.01411	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.01410	0.02021	1	0.02021	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.00517	0.01552	1	0.01552	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RC	0.20	0.00470	0.01411	1	0.01411	0.0	LN	0.0	125.	RC	38
RESISTOR ST=RN	0.20	0.01410	0.02021	2	0.05642	0.0	LN	0.0	125.	RN	43
RESISTOR ST=RN	0.20	0.10145	0.20291	1	0.20291	0.0	LN	0.0	125.	RN	40
RESISTOR ST=RC	0.20	0.00517	0.01552	1	0.01552	0.0	LN	0.0	125.	RC	38
CAPACITOR ST=CK	0.20	0.00739	0.01848	1	0.01848	0.0	LN	0.0	125.	CK	22
CAPACITOR ST=CS	0.20	0.00349	0.00873	1	0.00873	0.0	LN	0.0	85.	CS	32
CAPACITOR ST=CL	0.20	0.03223	0.19337	1	0.19337	0.0	LN	0.0	125.	CL	14
CAPACITOR ST=CK	0.20	0.00517	0.01293	2	0.02586	0.0	LN	0.0	125.	CK	22
CAPACITOR ST=CS	0.20	0.00420	0.01051	1	0.01051	0.0	LN	0.0	85.	CS	32
CAPACITOR ST=CL	0.20	0.03388	0.20325	2	0.40650	0.0	LN	0.0	125.	CL	14
CAPACITOR ST=CS	0.20	0.00159	0.00398	1	0.00398	0.0	LN	0.0	85.	CS	32
DIODE 1N5230B QUAL	0.20	0.00852	0.00516	1	0.00516	0.0	L	0.20	175.	L	54
DIODE 1N457 QUAL	0.20	0.00852	0.00516	1	0.00516	0.0	L	0.20	175.	L	54
LINEAR IC		0.07945	1.85792	1	1.85792	10.0	DI	0.0	22.		98
DIGITAL IC		0.21200	0.78954	1	0.78954	10.0	DI	0.0	4.		99
TRANSISTOR 2N2643 QUAL	0.20	0.01645	0.16449	1	0.16449	0.0	L	0.20	175.	L	61
TRANSISTOR 2N1893 QUAL	0.20	0.01645	0.16449	1	0.16449	0.0	L	0.20	175.	L	61
CAPACITOR ST=CK	0.20	0.01705	0.04263	1	0.04263	0.0	LN	0.0	125.	CK	22
TOTAL				51							

TOTAL FAILURE RATE (35.0 C) 6.60370

MTBF(HOURS) 151430.250
(17.31 YRS.)

FIGURE VI-4 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient temperature of 35 degrees C, and commercial grade quality.)

LEVEL 1

	STRESS RATIO (S)	ITEM FAILURE RATE	MS SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	DT C.	RL	BR2	GATES/ RATING T/RITR	STYLE/ MODEL	RT
DIGITAL IC		0.23329	0.01083	1	0.01083	10.0	D1	0.0	0.		99
DIGITAL IC		0.24769	0.03129	1	0.03129	10.0	D1	0.0	0.		99
DIGITAL IC		0.23329	0.01083	1	0.01083	10.0	D1	0.0	0.		99
DIODE 1N457	0.20	0.01123	0.11231	10	1.57235	0.0	L	0.20	175.	1N457	54
TRANSISTOR 2N4250	0.20	0.02954	0.29538	2	0.59077	0.0	L	0.20	175.	2N4250	60
TRANSISTOR 2N3566	0.20	0.01935	0.19346	1	0.19346	0.0	L	0.20	175.	2N3566	61
TRANSISTOR 2N6028	0.20	0.52432	5.24316	2	10.48633	0.0	L	0.20	175.	2N6028	96
CAPACITOR BT=CK	0.20	0.00434	0.01085	3	0.03254	0.0	LW	0.0	125.	CK	22
CAPACITOR BT=CB	0.20	0.00506	0.01266	1	0.01266	0.0	LW	0.0	85.	CB	32
CAPACITOR BT=CL	0.20	0.01167	0.07001	3	0.21004	0.0	MB	0.0	125.	CL	14
CAPACITOR BT=CB	0.20	0.00477	0.01192	1	0.01192	0.0	LW	0.0	85.	CB	32
CAPACITOR BT=CS	0.20	0.00278	0.00694	1	0.00694	0.0	LW	0.0	85.	CB	32
CAPACITOR BT=CL	0.20	0.03341	0.20040	1	0.20040	0.0	LW	0.0	125.	CL	14
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LW	0.0	125.	RN	43
RESISTOR BT=RW	0.20	0.11537	0.23075	2	0.46149	0.0	LW	0.0	125.	RW	40
RESISTOR BT=RC	0.20	0.00810	0.02429	2	0.04857	0.0	LW	0.0	125.	RC	38
RESISTOR BT=RN	0.20	0.01790	0.03580	3	0.10739	0.0	LW	0.0	125.	RN	43
RESISTOR BT=RW	0.20	0.11537	0.23075	3	0.69224	0.0	LW	0.0	125.	RW	40
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LW	0.0	125.	RN	43
RESISTOR BT=RW	0.20	0.11537	0.23075	1	0.23075	0.0	LW	0.0	125.	RW	40
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LW	0.0	125.	RN	43
RESISTOR BT=RX	0.20	0.11537	0.23075	1	0.23075	0.0	LW	0.0	125.	RW	40
TRANSISTOR 2N4250 QU=L	0.20	0.02954	0.29538	1	0.29538	0.0	L	0.20	175.	L	60
RESISTOR BT=RC	0.20	0.00810	0.02429	1	0.02429	0.0	LW	0.0	125.	RC	38
TOTAL				49							

TOTAL FAILURE RATE (50.0 C) 17.95885

MTBF(HOURS) 55682.8594
(6.36 YRS.)

FIGURE VI-5
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient of 50 degrees C, and commercial grade quality.)

LEVEL 2

	STRESS RATIO (S)	ITEM FAILURE RATE	NS SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	DT C.	RL	SR2	RATED/ RATING T/RIVS	STYLE/ MODEL	RT
DIODE 1N5305 QU=L	0.20	0.01123	0.11231	1	0.11231	0.0	L	0.20	175.	L	54
RESISTOR ST=RN	0.20	0.02165	0.04331	1	0.04331	30.0	LN	0.0	125.	RN	43
RESISTOR ST=RC	0.20	0.05997	0.17990	1	0.17990	30.0	LN	0.0	125.	RC	34
RESISTOR ST=RW	0.20	0.15149	0.30297	1	0.30297	30.0	LN	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.02399	0.07196	1	0.07196	30.0	LN	0.0	125.	RC	34
RESISTOR ST=RN	0.20	0.02165	0.04331	2	0.08662	30.0	LN	0.0	125.	RN	43
RESISTOR ST=RW	0.20	0.15149	0.30297	1	0.30297	30.0	LN	0.0	125.	RW	40
RESISTOR ST=RC	0.20	0.02638	0.07915	1	0.07915	30.0	LN	0.0	125.	RC	34
CAPACITOR ST=CB	0.20	0.01033	0.02582	2	0.05164	30.0	LN	0.0	85.	CB	32
CAPACITOR ST=CK	0.20	0.00828	0.02069	3	0.06207	30.0	LN	0.0	125.	CK	22
CAPACITOR ST=CL	0.20	0.06017	0.36100	1	0.36100	30.0	LN	0.0	125.	CL	14
TRANSISTOR NPN QU=L	0.20	0.01935	0.19346	1	0.19346	0.0	L	0.20	175.	NPN	61
LINEAR IC QU=D-1		2.75016	3.72062	1	3.72062	10.0	DI	0.0	28.	D-1	94
CAPACITOR ST=CB	0.20	0.00375	0.00937	1	0.00937	30.0	LN	0.0	85.	CB	32
RESISTOR ST=RN	0.20	0.02165	0.04331	1	0.04331	30.0	LN	0.0	125.	RN	43
CAPACITOR ST=CK	0.20	0.00468	0.01170	1	0.01170	30.0	LN	0.0	125.	CK	22
DIODE 1N2071 QU=L	0.20	0.01123	0.11231	1	0.11231	0.0	L	0.20	175.	L	54
TOTAL				21							

TOTAL FAILURE RATE (50.0 C) 9.75266

MTBF(HOURS) 173832.437
(19.87 YRS.)

FIGURE VI-5 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient of 50 degrees C, and commercial grade quality.)

LEVEL 3

	STRESS RATIO (S)	ITEM FAILURE RATE	NS SHIP FAILURE RATE	QTY	TOTAL FAILURE RATE	QT C.	RL	SR2	RATED/ RATING T/BIT8	STYLE/ MODEL	RT
RESISTOR BT=RN	0.20	0.01627	0.03254	5	0.16271	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RC	0.20	0.00810	0.02429	4	0.09714	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RW	0.20	0.11537	0.23075	1	0.23075	0.0	LN	0.0	125.	RW	40
RESISTOR BT=RC	0.20	0.00810	0.02429	1	0.02429	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RC	0.20	0.00890	0.02671	1	0.02671	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RC	0.20	0.00810	0.02429	2	0.09857	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RN	0.20	0.01796	0.03588	1	0.03588	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RW	0.20	0.11537	0.23075	2	0.46149	0.0	LN	0.0	125.	RW	40
RESISTOR BT=RW	0.20	0.11537	0.23075	7	1.61523	0.0	LN	0.0	125.	RW	40
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RC	0.20	0.00810	0.02429	1	0.02429	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RN	0.20	0.01627	0.03254	1	0.03254	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RC	0.20	0.00890	0.02671	1	0.02671	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RC	0.20	0.00810	0.02429	1	0.02429	0.0	LN	0.0	125.	RC	3A
RESISTOR BT=RN	0.20	0.01627	0.03254	2	0.06508	0.0	LN	0.0	125.	RN	43
RESISTOR BT=RW	0.20	0.11537	0.23075	1	0.23075	0.0	LN	0.0	125.	RW	40
RESISTOR BT=RC	0.20	0.00890	0.02671	1	0.02671	0.0	LN	0.0	125.	RC	3A
CAPACITOR BT=CK	0.20	0.00767	0.01919	1	0.01919	0.0	LN	0.0	125.	CK	22
CAPACITOR BT=CB	0.20	0.00401	0.01002	1	0.01002	0.0	LN	0.0	85.	CB	32
CAPACITOR BT=CL	0.20	0.01701	0.22204	1	0.22204	0.0	LN	0.0	125.	CL	14
CAPACITOR BT=CK	0.20	0.00537	0.01343	2	0.02686	0.0	LN	0.0	125.	CK	22
CAPACITOR BT=CB	0.20	0.00482	0.01206	1	0.01206	0.0	LN	0.0	85.	CB	32
CAPACITOR BT=CL	0.20	0.03090	0.23338	2	0.46677	0.0	LN	0.0	125.	CL	14
CAPACITOR BT=CB	0.20	0.00183	0.00457	1	0.00457	0.0	LN	0.0	85.	CB	32
DIODE 1N5231A QUAL	0.20	0.01123	0.11231	1	0.11231	0.0	L	0.20	175.	L	5A
DIODE 1N457 QUAL	0.20	0.01123	0.11231	1	0.11231	0.0	L	0.20	175.	L	5A
LINEAR IC		2.75016	3.72062	1	3.72062	10.0	DI	0.0	22.		98
DIGITAL IC		0.23329	0.61043	1	0.61043	10.0	DI	0.0	4.		99
TRANSISTOR 2N2483 QUAL	0.20	0.01935	0.19346	1	0.19346	0.0	L	0.20	175.	L	61
TRANSISTOR 2N1893 QUAL	0.20	0.01935	0.19346	1	0.19346	0.0	L	0.20	175.	L	61
CAPACITOR BT=CK	0.20	0.01771	0.04427	1	0.04427	0.0	LN	0.0	125.	CK	22
TOTAL				51							

TOTAL FAILURE RATE 0.10747
(50.0 C)

MTBF(HOURS) 166843.375
(12.99 YRS.)

FIGURE VI-5 (cont.)
Sample Group of Electronic Parts

(Failure rates calculated using MIL-Handbook 217 methods, Naval sheltered environment, ambient of 50 degrees C, and commercial grade quality.)

E.(3) The Effects of Higher Quality Levels

As previously indicated, commercial or "L" grade quality levels were used in developing failure rates. In order to determine the effects of using MIL grade components, the same 121 parts were run through the computer program using both lower level quality parts and MIL grade quality parts. The MIL grade parts used for this exercise were of the lower range of the total spectrum for MIL quality parts. Nevertheless, the failure rate dropped from 24.83 failures per million to 5.68 per million, or an improvement of 77 percent. Again, most of the improvement is due to semiconductors and ICs, which account for 75 percent of the improvement. Although resistors and capacitors constitute the majority of the parts, they only account for 25 percent of the improvement.

E.(4) Failure Rate Summary

To summarize, many factors influence the values of the failure rates. The basic failure rates used in this study are assumed to be the so-called unscheduled maintenance rates. The parts are assumed to be operating at an ambient temperature of 35° C., during the steady state phase, and are of commercial quality level. These failure rates can either be adjusted up or down by changing the basic assumptions regarding temperature, operational phase, maintenance, or quality levels. The degree of change varies by part type and class. Also, there are many unknowns as to the effect of these factors on non-electronic parts, and many of the factors had to be estimated. Table VI- summarizes the general effects of these four factors. By increasing the temperature from 35° C. to 50° C., the basic failure rate generally increases; however, for hardware such as valves and pumps, the temperature change should not have a substantial effect and the factors are assumed to be 1. The overall factor for change in temperature is 1.2.

For quality, changing from commercial to military grades will reduce failure rates. Little data could be found on non-electronic parts. However, a significant reduction is exhibited using MIL-Handbook calculations for electronic parts, The adjusted failure rate for use of military level parts is 0.71 of the base failure rate.

The premature failure rates are significantly higher than those for the steady state, and converting from steady state to premature state increases the failure rate on the average by 7.9.

The adjustment to the base failure rate due to maintenance and tests is on average 0.48 percent of the base rate. In other

TABLE VI-3
FAILURE RATE FACTOR SUMMARY TABLE

	PART CLASS	BASIC RATE 10-6	FACTOR TEMPERATURE	QUALITY FACTOR	PREMATURE FACTOR	MAINTENANCE FACTOR
1.	Actuators	7.67	1.0*	.9*	6.6	.46
2.	Connectors	0.05	1.4	.48	6.6	.44
3.	Controls, Pneumatic (sample controller)	2.92	1.0*	.9*	6.6	.46
4.	Controls, Electronics (sample circuit of 121 parts)	24.83	1.32	.22	3.25	.80*
5.	Power Supplies	9.26	1.32	.22	3.25	.80*
6.	Pumps	59.64	1.0*	.9*	11.6	.40
7.	Regulators	19.65	1.0**	.9*	6.6	.46
8.	Relays	1.06	1.18	.5*	6.6	.30
9.	Switches	7.08	1.18	.5*	6.6	.44
10.	Transducers/Sensors	20.95	1.3*	.8*	6.6	.44
11.	Valves, Pneumatic	32.75	1.0*	.9*	11.6	.46
12.	Valves, Hydraulic	18.59	1.0*	.9*	11.6	.46
13.	Valves, Solenoid	38.41	1.0*	.9*	11.6	.46
14.	Valves, Without Operators	12.07	1.0*	.9*	11.6	.31
	AVERAGE		1.2	0.71	7.9	.48

*Estimated Factors

words, approximately half of all failures can be eliminated through adequate preventative maintenance and tests. The remaining failures probably cannot be eliminated because they are undetectable and/or fail instantaneously. The 0.48 improvement factor due to maintenance correlates very closely with data generated on other large complex systems. It has been found in studies of historical data on military systems that, on the average, there is a one to one ratio of failures that have degraded to the point that they effect the function of the equipment to failures that are found prior to degrading to the point of being a functional failure. The degree to which the non-operational type of degradation can be eliminated prior to total failure is a function of the effectiveness of inspection, tests, and preventative maintenance programs

VII. FAILURE MODES AND EFFECTS ANALYSES (FMEA)

During the Task II effort, Failure Modes and Effects Analyses (FMEA's) were conducted down to the part level (transistor, integrated circuit, control valve, etc.). The completed FMEA sheets for Ships A, B, and C are provided in Appendices B, C, and D. In the subsections which follow, the FMEA approach is described and failure modes are discussed.

A. FMEA APPROACH

The basic, overall approach to the FMEA's for all three ships was first to subdivide the hardware into realistic, manageable groupings. At the "top level," these groupings constitute the subsystems, or major functional areas. These subsystem groupings for each ship are listed at the end of this section.

The hardware within each subsystem was then further subdivided by examining the individual hardware elements. Groupings were established based on the subfunctions performed. In some cases, from three or four to a dozen or so elements could be grouped together into one subfunction. In other cases, no grouping was found possible, and individual elements (for instance, a NAND gate) were considered as a "group." In all cases, these groupings were developed from schematics, and were based on the criterion that each element within the group contribute to the same failure effect.

One example of this grouping would involve a circuit, such as a relay driver, with only one subfunction. While the driver is composed of several parts, it can be reasonably assumed that failures within the driver would have the same overall effect, namely to cause the associated relay to energize or de-energize incorrectly. In this example, the parts within the relay driver form a subgroup.

Another example would involve an element having an output used in more than one place. In this example, potential element failure modes would contribute to failure effects in each area where the output was used. It could thus not be grouped together with any one area where its output was used since its potential failure modes would also effect other areas. Rather, it would form its own unique "group." Logic gates often exhibit this type of failure effect and form "groups" of a single element each.

Each of these groups or single elements, as appropriate, were entered into the FMEA worksheets. It can be seen, therefore, that the FMEA's cover all hardware elements.

Once the hardware had been subdivided, the failure modes for each grouping were entered into the FMEA worksheets. These failure modes are discussed in detail below, but generally include failures to the extremes of each group's operating boundaries. These "extremes" include fail high/low or fail true/false for digital logic, contact stays open/closed for relays, signal stays active/never active, etc.

For each group, the subsystem and system failure effects for each potential failure mode were then determined. The subsystem failure effects constitute the impact of the failure mode on subsystem operation, and their entries on the FMEA worksheets describe the abnormal subsystem operation that would occur as a result of the failure mode under consideration. Likewise, the system failure effect entry describes the abnormal operation that would occur at the overall system level due to the failure mode. As an example, assume that the failure mode under consideration was "output signal stays active" for a particular relay driver. Then the subsystem failure effect would be that the associated relay stays energized. At the system level, the failure effect would be that the associated function stays in the operating mode dictated by the energized state of the relay (for instance, feedwater pump stays on).

The FMEA approach described thus far is basically the standard approach taken to any FMEA. In addition, DOVAP covered three other areas that are not necessarily included, per se, in all FMEA's. These areas were included for later use in the criticality analyses, and are as follows:

First, where applicable, cross reference numbers were made on the FMEA worksheets to the criticality sheets to identify any means available for detecting the failure mode under consideration. These failure detection means primarily involve alarms and such visual indications as gauges.

Second, any back-up provisions for manually overcoming the effects of the failure modes were identified for cross-reference to the criticality sheet. Such back-up provisions include manual operation of a valve, local control from a remote station, handpump control of hydraulics, etc.

And third, failure rates for all FMEA entries were provided on the worksheets. These failure rates cover the part(s) in each subgrouping, and are also apportioned to the failure modes under consideration. For instance, assume that the failure modes for a particular relay are "contact stays open" and "contact stays closed," and that it has been determined that these failure modes are equally likely. This implies that if the relay fails, there is a 50 percent chance that its contact

will stay open and 50 percent that it will stay closed. Therefore, 50 percent of the relay's total failure rate is apportioned to each potential failure mode.

B. FAILURE MODES

The degree of realism achieved through a failure modes and effects analysis depends significantly on the realism of the failure modes considered. This occurs because the failure effects identified in an FMEA are a direct function of the failure modes assigned to the various hardware groupings.

There are two basic sources of failure mode information for use in an FMEA. The first source is published failure mode data and compendiums; the second is the application of engineering experience.

The major problem with published failure mode data is that it is severely limited. Many individual papers cite some particular failure mode(s) observed in operation, and such information from the Task I literature search was used during Task II of this study. On the whole, however, failure mode information of this type is not comprehensive, and at best can only serve to verify data obtained from other sources.

There are a few published compendiums containing failure mode information, and three were used on this study. While these do provide reasonably comprehensive data, they are limited in the hardware areas they cover.

Of the three sources, the "SRI data"(2) was used for background information on mechanical, and especially pneumatic hardware. Since the failure modes given in this source are based on operating data from nuclear power plants, it is not clear that the data is representative of failure modes in a marine environment. Nevertheless, failure modes for control equipment are briefly described, and the number of occurrences given. This information was used in Task II to serve as "guidelines."

The second source (3) involves a quite comprehensive study conducted by RADC on electronic part failure modes, but since it was performed some time ago it provides no data on integrated circuits. The data it does provide on transistors, capacitors, and the like still appears valid since it is difficult to ima-

(2) Failure Rate Source VI.A. (2), page VI-I
(3) Failure Rate Source VI.A. (1), page VI-I

gine that such parts would have developed any totally new failure modes in the period since the study was performed. Hence, DOVAP relied heavily on this study for electronic part failure mode types and frequencies.

The third source (4), also from RADC, is primarily a compendium of non-electronic part failure rates, but some failure mode information is also given. Since a large amount of this data is based on military applications, it was used during this study, as was the SRI data, to serve as guidelines.

In establishing the failure modes to be considered in an FMEA, engineering experience traditionally plays a significant role. This occurs in part because of the limitations associated with published data. It also occurs because "real life" failure modes are often not amenable to the FMEA approach.

For instance, intermittent failures and "glitches" of various types are common in actual operations, and their causes are often never determined. Also, in practice, parts are often replaced not because they have totally failed but rather because they have degraded to the extent of effecting system operation. In addition, integrated circuits present tremendously complicated failure mode possibilities. Typical causes of integrated circuit failures include substrate fractures, internal shorts across conductors, internal voids or holes, etc. The manner in which such failure mechanisms impact circuit operation depends on the nature and location of the defect. Some defects will produce quite straightforward failure modes (e.g., circuit output shorted to ground). Others can cause malfunctions in up to every circuit on the ship.

In view of such "real life" characteristics, as well as the limitations of published data, obtaining failure modes amenable to the FMEA approach requires assumptions based on engineering experience. The basic assumption usually made, and the one DOVAP applied on this study, is that parts fail to their extremes in either direction.

The disadvantage of this assumption is that it only partially reflects "real life." That is, some failures will indeed involve these extreme failure modes, while others will involve failure modes somewhere "in between." The advantage of this assumption, and it is a significant one for this study, is that the resulting FMEA will represent the worst case boundaries. This implies that it is not likely that a "more worst case" condition could occur than was revealed in the FMEA.

(4) Failure Rate Source VI.A. (3), page VI-2

C. FMEA EXAMPLE

In the paragraphs which follow, an example from the Task II FMEA's is described in order to illustrate approach and procedures. The example covers a portion of digital logic used for control of a boiler Master Fuel Oil Valve.

A sample of the completed FMEA worksheets for this portion of the digital logic is provided in Figure VII-2. A simplified schematic of this logic is shown in Figure VII-1. Since the logic is implemented with Integrated circuit NAND-NOR gates, the Figure VII-1 schematic is highly simplified. For instance, the recirculation latch shown actually incorporates several gating stages so that the logic inversions at each gate are combined properly to obtain the correct logic level at the output. The circuitry shown in the figure and covered in the sample FMEA worksheets functions as follows.

The Master Fuel Oil Valve stays open as long as its solenoid is energized. The solenoid driver contains a power driver at its output stage such that when the transistors in the power driver conduct, the solenoid is energized. When the power driver transistors are not conducting, the solenoid de-energizes and the Master Fuel Oil Valve closes. Thus, the opening and closing of the Master Fuel Oil Valve is achieved by "switching" the power driver transistors on or off.

This, in turn, is accomplished during steady state operations by the "Open Mst F.O. Valve Command." This command stays active as long as no boiler trips are present. If a boiler trip condition is detected, the command goes "false", thus switching off the power driver transistors and de-energizing the solenoid.

An open command can also be generated by manually setting the recirculation latch via the Master Fuel Oil Valve Reset pushbutton. This allows fuel oil to be recirculated under manual control. The recirculation latch will reset, however, at the start of a purge cycle or if any burner valve is open.

Open commands are passed on to the solenoid driver only when the manual trip latch is reset. Thus, if it is desired to manually trip the Master Fuel Oil Valve, the Master Fuel Oil Valve Trip pushbutton is depressed, which in turn, sets the Manual Trip Latch. Recovery following a manual trip requires that the Master Fuel Oil Valve Reset button be depressed.

From this brief description, several failure effects can be readily noted. If the solenoid driver stays energized, the Master Fuel Oil Valve will remain open. This can occur if the solenoid driver fails such that its power driver transistors always conduct. This can be caused by several part failure modes within the driver circuit itself. It can also be caused if the AND gate that switches the solenoid driver fails such

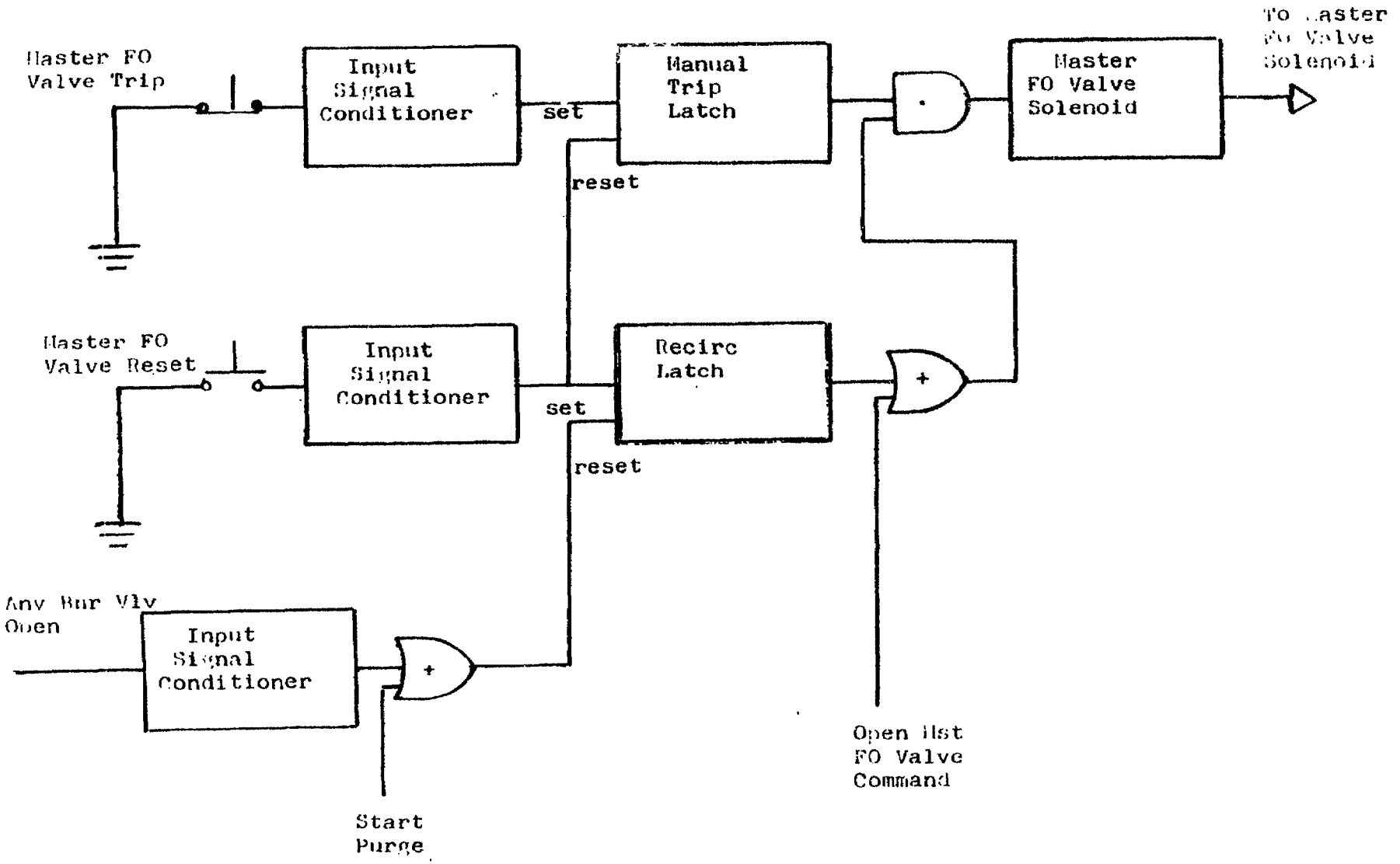


Figure VII-1

Simplified Schematic of Logic Covered in FIEA Sample Sheets

FIGURE VII-2
Sample of FMEA Worksheets

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

SHEET: 2 OF 19

SUBSYSTEM: 1.1.3 Boiler Safety

PREPARED BY: REV DATE:

REF NO.	ITEM NOMENCLATURE & FUNCTION	FAILURE MODE/S	FAILURE EFFECT SUBSYSTEM	FAILURE EFFECT SYSTEM	TOTAL UNSCHED MAINT ACTNS MAN HOURS		Failure Mode Ratio	COMMENTS/COMPENSATING PROVISIONS
2A.	Master Fuel Valve Solenoid Driver Ckt: - 1 Resistor, Film, Type RN - 2 Resistors RCR - 1 Resistor, WW, "915-2A - 3 Diodes, Power, JANIN 3611 - 1 Transistor, PNP Power, "2N6058-1 - 1 Transistor, NPN, Darlington, "MPS-A14 - 1 LED - 1 AND Gate, ¼ of IC P/N CD4081BE - 1 Inverter, ¼ of IC P/N CD4049AE	Stays true	Master Fuel Valve would stay energized (i.e, open)	Boiler could not be tripped via Master Fuel Valve automatically. Trips would still shut down burner valves			.50	Master Fuel Valve can be jacked open and closed by hand
2B.		Stays false	Master Fuel Valve deenergizes (i.e, closes)	Boiler Flame out; Boiler Trip would also occur if Trip circuitry non-failed			.50	Detection via F.O. to Burner Pressure Alarm or flame intensity indicators.

Figure VII-2 (Cont.)

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

SHEET: 3 OF 14

SUBSYSTEM: 1.1.3 Boiler Safety PREPARED BY: REV DATE:

REF NO.	ITEM NOMENCLATURE & FUNCTION	FAILURE MODES	FAILURE EFFECT: SUBSYSTEM	FAILURE EFFECT: SYSTEM	TOTAL MAINT ACTNS		Failure Rate Source	COMMENTS/COMPENSATING PROVISIONS
					MAN HRS/MA			
3A.	Manual Trip Latch:	Stays set	Same as 2B (Logic "thinks" it received manual trip signal)	Same as 2B			.5e	Same as 2B
	- 1 Resistor, Film, Type RN							
	- 1 Capacitor, Film, .33K051102-3							
	- 2 NOR Gates, ¼ of IC P/N CD4001AE							
	- 1 Inverter, ¼ of IC P/N CD4049AE							
3B.		Stays Reset	Master F.O. Valve could not be tripped via manual trip switch	Lose Backup manual boiler trip capability			.5e	Same as 2A
4A.	Mst FO Vlv Trip PB Input ckt:	Stays true	Same as 2B (same as 3A)	Same as 2B			.5e	Same as 2B
	- 3 Resistors, Film, Type RN							
	- 1 Capacitor, Type CL							
4B.	- 1 Switch, PB	Stays False	Same as 3B	Same as 3B			.5e	Same as 3A
5A.	Mst FO Vlv Reset PB Input Ckt	Stays true	Manual trip latch stays reset & Reset latch stays set. Master FO Valve will stay open	Same as 2A			.5e	Same as 2A
	- Same parts count as for item 4 -							

Figure VII-2 (Cont.)

FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

SUBSYSTEM: 1.1.3 Boiler Safety — PREPARED BY: _____ REV _____ DATE: _____ SHEET: 4 OF 19

REF NO.	ITEM NOMENCLATURE & FUNCTION	FAILURE MODE/S	FAILURE EFFECT: SUBSYSTEM	FAILURE EFFECT: SYSTEM	TOTAL MISSION MAINT ACTNS: MAINT ACTNS	TOTAL MISSION MAINT ACTNS:	Failure Rate Percent	COMMENTS/COMPENSATING PROVISIONS
5B.	Mst Fo Vlv Reset PB ckt (cont)	Stays false	Lose switch function (i.e., Fo Recirculation)	Mst F.O. Valve could not be opened manually via Reset switch for F.O. Recirculation			.50	Same as 2A
6A.	All Burner Valves Closed Input circuit: -2 Resistors, Film, Type RN -1 Diode, Zener, IN5242 -1 Schmitt Trigger, ¼ of IC P/N CD4010BBF	Stays true	All Burner Valves would appear closed; Recirc latch would stay reset; Loss Mst Fo Valve Reset PB function - same as 5B	Same as 5B			.50	Same as 2A
6B.		Stays false	Recirc latch would not reset if any burner valve opened; Mst Fo Vlv Reset PB would not be inhibited if a burner valve opened	Recirculation could be manually commanded with a burner valve open - safety hazard. There is a redundant signal that protects against this - see item 13.			.50	

that its output always appears "true."

Conversely, if a failure causes the solenoid to de-energize, the Master Fuel Oil Valve will close and the boiler will shut down. This can occur if the power driver transistors stop conducting, and can be caused by certain part failure modes within the driver circuit. It can also be caused if the AND gate switching the solenoid driver fails such that its output always appears "false."

A failure characteristic typical in digital circuitry can also be seen from this example. That is, failures "back down the line" can propagate through the logic and cause some of the same failure effects as those at the output stages. For instance, if the input signal conditioner circuit for the "Master F.O. Valve Trip Pushbutton" input failed such that the input signal appeared "true" (or, in other words, the pushbutton appeared to be depressed), the Manual Trip Latch would be set, the solenoid driver would "switch off," and the Master Fuel Valve would close and shut down the boiler.

D. FMEA POINTS OF INTEREST

From approximately 150 to 400 system-level failure effects were revealed by the FMEA's for each system. For Ship A, which has the most complex control system, the FMEA revealed about 400 system failure effects. For Ship B, which has the next most complex control system, about 200 system failure effects were identified. Ship C has the least complex control system but the various operating mode and control station provisions increase the number of system failure effects; about 150 were identified. Many of these failure effects are insignificant. For all three ships, however, a considerable number have direct or indirect safety implications, and these are depicted in the fault trees.

As just indicated, the FMEA results were utilized in the fault trees. They were also utilized in all other study analyses. They form the basis for the criticality analysis, as discussed in Section IX. They were extensively utilized in developing the reliability criteria described in Section X. Reliability predictions were computed from the parts groupings established for the FMEA's. FMEA results were also considered in the maintenance analysis.

Since the FMEA's constitute the basis for other study activities, two points must be addressed. The first concerns the degree of realism achieved in the FMEA's; the second, the degree of comparability between the three ships.

D.(1) FMEA Realism

As indicated earlier, the FMEA's were based on extreme failure modes (e.g., fail open/fail short, fail active/fail inactive, etc.). Therefore, to assess the realism of the FMEA's, the realism of such failure modes must be considered.

Both data and experience from aerospace programs indicate that roughly one-fourth of all failures involve these extreme failure modes. However, the parts used on aerospace programs are generally of a consistently higher quality than was found to be the case during this study. These higher quality levels imply that many design and manufacturing defects contributing to extreme failure modes have been eliminated. For the lower quality level parts that are so extensively utilized in the systems evaluated during this study, defects contributing to extreme failure modes are much more likely. Based on past experience and consideration of actual problems that have occurred in engine room automation systems, it seems reasonable to estimate that over 50 or 60 percent of all failures would involve extreme failure modes.

The remaining failure modes would involve intermittents, degradation, etc. Some of these would cause, if only momentarily, the same effects as would an extreme failure mode. For instance, an intermittent could involve a short-term, fail-short condition. It is difficult to estimate the percentage of failure modes that could manifest these effects, but 15 percent would seem extremely low.

Thus, considerably under 25 percent of the failures would involve "real life" failure modes that were neither extreme nor manifested in the same effects as those for extreme failure modes. Since, as indicated earlier, the FMEA's reflect worst case boundaries, the effects of these types of failure modes can be reasonably expected to lie "somewhere between" the failure effects delineated in the FMEA's. That is, they should certainly not introduce any effects "worse" than those already identified in the FMEA's.

D.(2) FMEA Comparability

An overall ground rule for the study was that analytical results for the three ships be directly comparable. To this end, the FMEA's for all three ships utilized the same approach and the same failure modes. Differences in the FMEA's are, therefore, due to differences in the design approach and implementation of the control systems.

Differences in the control systems, and hence the FMEA's, for Ships A and B (the two steam vessels) are due to two factors. First, the design approach differs, with Ship A utilizing a hybrid digital/pneumatic system, while Ship B utilizes a hy-

brid digital/analog system. Second, the digital logic on Ship A is significantly more complicated than that on Ship B, with a concomitant increase in the number and complexity of the failure effects. The control system on Ship C (the diesel vessel) obviously differs from those on Ships A and B. Tables VII-1, VII-2 and VII-3 gives the subsystem breakdown for the three ships and the associated reference numbers used in the FMEA.

Except for the differences dictated by the different control system design approaches, there is only one other minor difference in the FMEA's for the three ships, and this is a function of implementation. On Ship A, more parts could be grouped together than on Ship B, and, to a lesser extent, than on Ship C. The FMEA entries for Ships B and C consist of a large number of single parts, primarily logic gates. The failure modes considered for these gates were fail high/fail low.

On Ship A, a large number of FMEA entries involve several parts that could be grouped together as discussed above. Groups involving a "chain" with an input circuit, inverter, and a gate or two occur quite frequently. It is not accurate in such a group to speak of "fail high" or "fail low" failure modes because a signal that "failed high" at one point in the chain would be equivalent to one that "failed low" on the other side of an inverting logic element. Thus, the failure modes considered were "fail true" and "fail false," where the distinction between "true" and "false" was based on the purpose of the group of elements. A signal whose purpose, for instance, is to indicate that all burner valves are closed, was considered to have "failed true" when the failure made it appear that all burner valves were closed. It was considered to have "failed false" when the failure indicated that all burner valves were not closed. The failure effects identified through these true/false failure modes would be identical to those identified if each element in the chain had individually been considered to have failed high/low.

None of these differences impact the comparability of the FMEA's. While each ship's FMEA identifies failure effects similar or identical to those on the other ships, each FMEA also contains a number of failure effects unique to each particular system. These differences in failure effects simply reflect different design and implementation approaches.

TABLE VII-1
Ship A Subsystem Breakdown

1.0 Boiler Control
- 1.1 Load and Combustion Control
  - 1.1.1 Purge Control
  - 1.1.2 Prelight Control
  - 1.1.3 Boiler Safety Logic
  - 1.1.4 Burner Logic
  - 1.1.5 Burner Demand Sequencing
  - 1.1.6 Combustion Air Control
  - 1.1.7 Fuel Oil Control
    - 1.1.7.1 Fuel Oil Flow Control
    - 1.1.7.2 Fuel Oil Temperature and Pressure Control
    - 1.1.7.3 Fuel Oil Supply Control
  - 1.1.8 Feedwater/Drum Level Control
  - 1.1.9 Master Load Control
- 1.2 Boiler Local Panel

2.0 Superheated Steam Temperature Control

3.0 Desuperheated Steam Control (including Atomizing and Gland Steam)

4.0 Exhaust and Bleed Steam Control

5.0 Low Pressure Steam Generator Control

6.0 Third and Fourth Stage Feed Heater Control

7.0 Lube Oil Control

8.0 Condensate System Control

9.0 Miscellaneous Alarms and Indications

10.0 Main Engine Control

TABLE VII-2
Ship B Subsystem Breakdown

1.0 Burner Management, Master

2.0 Burner Module

3.0 Combustion Control, Boiler Demand Logic

4.0 Combustion Control

6.0 Drum Level Control

7.0 Feedwater Control

8.0 Feedwater Recirculation Valve Control

9.0 Superheated Steam Temperature Control

10.0 Steam Dump Control

11.0 Forward Feedpump Start/Stop Control Module

12.0 Fuel Oil Header Temperature

13.0 F.O. Recirculation Control

14.0 L.O. Pump Controls

TABLE VII-3
Ship C Subsystem Breakdown

1.0 Station in Control Logic
- 1.1 Control Transfer Logic
- 1.2 Control Transfer Input Interface
- 1.3 Control Transfer Output Interface

2.0 Propulsion Control
- 2.1 Engine and Clutch Control Logic
- 2.2 Engine and Clutch Control Input Interface
- 2.3 Engine and Clutch Control Output Interface

3.0 Mode Control
- 3.1 Mode Control Logic
- 3.2 Mode Control Input Interface
- 3.3 Mode Control Output Interface

4.0 Pitch Control
- 4.1 Pitch Controller
- 4.2 Pitch Controller Input Interface
- 4.3 Pitch Controller Output Interface
- 4.4 Pitch Cutback
- 4.5 Pitch Cutback Input Interface

VIII. FAULT TREE ANALYSIS

A. GENERAL DISCUSSION

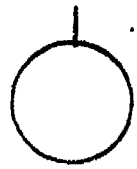
Fault tree analysis is a systematic method for acquiring information concerning abnormal behavior of a subsystem. The initial process in the fault tree analysis is to determine one or more undesirable events that abnormal behavior of the system could possibly produce. Each event is then individually analyzed to determine its possible causes. The undesirable system events constitute the top-level events in a fault tree diagram. This diagram constitutes a graphical model of the parallel and sequential combinations of faults which could cause the occurrence of each pre-defined top-level undesirable event.

The fault tree diagram is an arrangement of logical elements known as "gates" which permit or inhibit the passage of fault conditions up the tree. In other words, the gates show the relationship of events needed for the occurrence of higher events. The higher event is the output of the gate, lower events are the inputs into the gate. The gate symbols denote the type of relationship required for the input events to produce the output event. Standard symbology has been adopted for the construction of fault trees, and the logic symbols used during this study are as follows:

A.(1) Primary Events

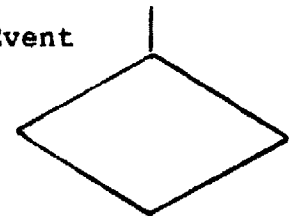
Primary fault tree events are those which, for one reason or another, have not been further developed. For these primary events, probabilities have been determined. Four types of primary events were used in this study. They are:

A.(1)(a) The Basic Event



The circle describes a basic, initiating fault event that requires no further development, and signifies that the appropriate limit of resolution has been reached. Events represented by circles are either component failures or groups of component failures, and form the bottom-most levels of the fault tree diagrams.

A.(1)(b) The Undeveloped Event

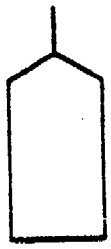


The diamond describes a specific event that is not further developed either 1) because the event is of insufficient consequence or 2) because information relevant to the event is unavailable. In most cases, diamonds represent failures or conditions outside of the scope of this study, such as conditions involving crew actions or hardware failures outside the control systems. Probabilities were assigned to events represented by diamonds in order to obtain more meaningful probabilities of the top-level events.

A.(1)(c) The Conditioning Event

The ellipse is used to record any conditions or restrictions that apply to a logic gate. It is used in this study to qualify when certain events occur, e.g., during low demand, during maneuvering, etc.

A.(1)(d) The External Event

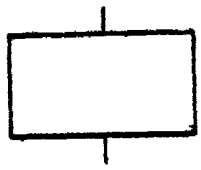


The house is used to signify an event that is normally expected to occur: e.g., fuel oil is available when needed. Thus, the house symbol displays events that are not, of themselves, faults.

A.(2) Intermediate Events

An intermediate event is a fault condition or contributing factor occurring because one or more preceding events require

further definition prior to an input logic gate. All intermediate events are symbolized by rectangles, i.e.,

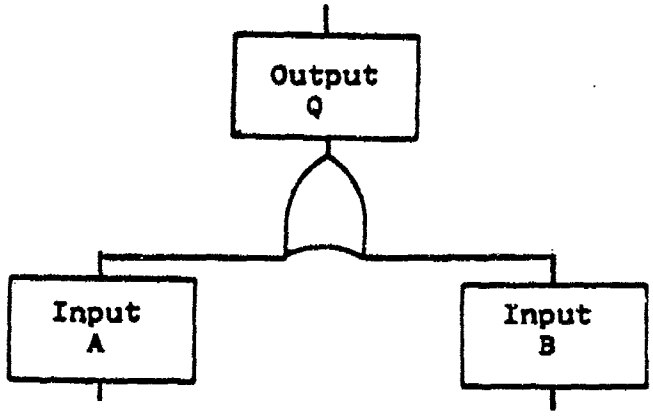


A.(3) GATES

Two basic fault tree gates were used in this analysis: the OR-gate and the AND-gate. The inhibit gate, a variant of the AND-gate, was also used.

A.(3)(a) The OR-Gate

The OR-gate is used to show that the output event occurs if one or more of the input events occur. There may be any number of input events to an OR-gate. The figure below shows a typical two-input OR-gate with input events A and B,and output event Q. Event Q occurs if A occurs or B occurs.

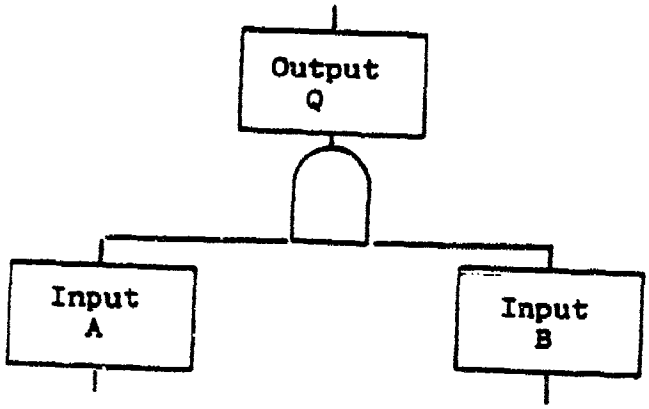


THE OR-GATE

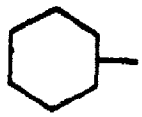
A.(3)(b) The AND-Gate

The AND-gate is used to show that the output fault occurs

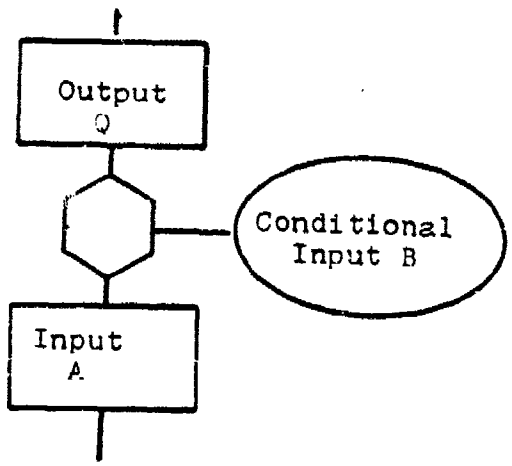
only if all input faults occur. There may be any number of input faults to an AND-gate. The figure below shows a typical two-input AND-gate with input events A and B, and output event Q. Event Q occurs only if events A and B both occur.



A.(3)(c) The INHIBIT-Gate



The INHIBIT-gate, represented by the hexagon, is a special case of the AND-gate. The output is caused by a single input, but some qualifying condition must be satisfied before the input can produce the output. The qualifying condition is termed the conditional input, and is described within an ellipse drawn to the right of the inhibit gate. The figue below shows a typical INHIBIT-gate with input A, conditional input B and output Q. Event Q occurs only if input A occurs under the condition specified by input B.



A.(4) Transfers Within The Fault Tree

Transfers within a fault tree are used as a matter of convenience to avoid extensive duplication or to continue the fault tree diagram on another page. Triangles are used to indicate tranfer symbols. A line from the apex of the triangle denotes a "transfer in", and a line from the side, a "transfer out". A "transfer in" attached to a gate will link to its corresponding "transfer out". This "transfer out", perhaps on another sheet of paper, will contain a further portion of the tree describing input to the gate. All transfer symbols are numbered so that the inputs/outputs can be traced. In some cases, such as for "manual intervention", the same branch of the tree is used repetitively. In these cases the branch is only drawn once, although the transfer in symbol is shown many times.

A.(5) Construction Rules

Certain rules were used in the construction of the fault trees and these are as follows:

a) Each statement entered into an event box is a description of a fault. This description states what the fault is and when it occurs.

b) Faults are either component faults or system faults. Component faults are, obviously, the result of a component failure. If the fault is not the result of a component failure, it is then classified as a "state of the system fault." For component faults, the failure is the primary event. For a "state of the system faults," the causes are identified with further gates.

c) If a failure can be inhibited by a second failure, it was assumed that the second failure does not occur and that the first failure was therefore not inhibited. In other words, it was assumed that if a normally functioning component could propagate a fault, it would not fail such as to inhibit further development of the fault.

The fault tree procedures as described above provide a logical sequence for pictorially describing the series of events contributing to the top-level faults or undesirable events. From this pictorial depiction, fault trees can be qualitatively evaluated. They can also be quantitatively evaluated through a process described in the following paragraphs.

B. QUANTITATIVE FAULT TREE ANALYSIS THROUGH BOOLEAN ALGEBRA

By applying the principals of Boolean algebra, fault tree pictorial representations of events can be translated to quantitative values. This can be accomplished through expressing the top events of a fault tree in terms of their Boolean relationships to the lower level fault events. However, before this mathematical analogy can be shown, an explanation of the rules of Boolean algebra is necessary.

B.(1) Rules of Boolean Algebra

As previously discussed, the two basic gate categories are the OR-gate and the AND-gate, and these pictorially relate fault tree events to Boolean algebra operations discussed above. Each gate has one output and one or more inputs. For an OR gate, the Boolean operator is denoted by the "+". Thus an OR gate with inputs A and B and output Q would be represented in Boolean terms as:

$$Q = A + B$$

Since probabilities are dealt with in fault trees, the probability of Q is the probability of A OR the probability of B. If the probabilities are quite small (much less than 10%) the expression becomes:

$$P_Q = P_A + P_B$$

If the probabilities are not small, a qualifying term must be included, and the OR expression becomes:

$$P_Q = (P_A + P_B)(1 - P_A P_B)$$

For fault trees such as those developed during the DOVAP study, probabilities are developed from the part failure rates. Recall from section II that the reliability R, of an equipment is the probability that it will not fail. The probability that it will fail is therefore:

$$P = 1 - R, \text{ or } 1 - e^{-\lambda t}$$

and such probabilities can be "plugged into" Boolean expressions.

For an AND gate, the Boolean operator is denoted by the ".". Thus an AND gate with inputs A and B and output Q would be represented in Boolean terms as:

$$Q = (A)(B)$$

Again, since probabilities are dealt with in the fault trees, the expression becomes

$$P_Q = (P_A)(P_B)$$

The AND and OR operators in Boolean algebra are manipulated exactly as in ordinary algebra. Thus, if P_A was 3 percent and P_B was 2 percent, the OR expression would be:

$$P_Q = 0.03 + 0.02 = 0.05 = 5\%,$$

or, in other words, Q would have a probability of occurrence of 5 percent. The AND situation would be expressed as:

$$P_Q = (0.03)(0.02) = 0.0004 = 0.04\%,$$

or, in other words, Q would have a probability of occurrence of four-hundredths of a percent.

There are far more types of manipulatons possible with Boolean algebra per se, and with its application to fault trees. However, the fault tree analysis on the DOVAP study had no occasion to go beyond the straight forward AND-OR relationships described above. For further information or more complicated fault tree manipulations, the reader is referred to "Fault Tree Handbook", published by the U.S. Nuclear Regulatory Commission, NUREG-0492, January, 1981, as a good source of information.

C. FAULT TREE MODELS AND ASSUMPTIONS

Fault tree analyses describe analytically the undesired states of the systems, and all credible ways in which the undesired events can occur. The fault trees are graphic models of the various parallel and sequential combinations of faults that will result in the occurrence of the predefined undesired event.

For the fault trees developed during this study, the top undesirable events were defined in the Statement of Work. Due to the basic differences between diesel and steam systems, the top, undesirable events are somewhat different for the two types of systems. For the steam system, the following are the top undesirable events:

a) Unscheduled propulsion system shutdown due to automation control failures

b) Loss of turbine RPM control due to automation control failures.

c) Loss of directional control due to automation control failures.

For the diesel system, the following are the top events:

a) Vessel does not maintain way as commanded.

b) Vessel does not respond correctly to speed/direction change commands.

c) Uncommanded speed/direction changes.

For the steam systems the top level unscheduled shutdown was further divided into shutdowns due to either boiler or turbine shutdowns and shutdowns due to either boiler over-pressure or explosion. The fault trees for all 3 systems are presented in Appendix E.

Because of the complexity of the evaluations, certain assumptions had to be made. These assumptions are based on the most likely events and may not be 100 percent correct. However, they appear reasonable for this study.

One assumption is that component failures are independent. Common cause failures, that is, those where a single failure can cause several failure modes, were not evaluated. The effort required to identify common cause failures and failure modes would require a separate study by itself.

Manual backup or efforts are represented by one branch of the logic tree, and this is repeated for each occasion where manual intervention could take place. This sub-tree covers the situation where manual intervention could preclude a fault. Such intervention would not be effective if the alarm fails, and therefore does not alert the crew, or if the alarm sounds but crew action is inadequate.

In order to emphasize the tremendous importance of the crew taking the proper corrective action, the fault trees were calculated twice, once with the crew action never being correct, and the second time with the crew's action correct 90 percent of the time. The true probability of the crew performing the correct action is probably somewhere between 50 and 90 percent but there is no data to substantiate this.

The quantitative evaluation of explosions as related to the top undesirable events became nebulous. Explosions can

range anywhere from a slight chimney puff to severe boiler damage and possible injury or death to crew members. Most explosions are the result of a series of undesirable faults, some of which cannot be controlled by the automation system. Also, explosions can result in considerable secondary damage. Therefore, it was assumed that the top most fault resulting from explosions would be that the turbine would be shutdown to assess and repair damage.

In general, the quantitative estimates of the fault tree analysis are on the pessimistic side. The fault trees contain many AND conditions representative of a combination of the control system functions and other turbine or boiler hardware failures. Because these combination-type events were so interrelated with the top undesirable events, it was felt that such occurrences involving non-control functions should be included rather than assuming that they would not occur. As an example, the possibility of turbine damage due to high vibration is the probability that the turbine high vibration trip mechanism does not work and the occurrence of high turbine vibration levels. This is an AND condition, where the two events must occur. The probability of high vibration levels could not be determined during this study and, therefore, a value had to be assumed. Again, the vibration is not a function of the automated control system; however, the combined event directly relates to the possibility of damage to the turbine.

The probabilities of boiler damage as well as turbine damage are also on the pessimistic side. In most cases, damage resulting from control system failures is not instantaneous. Usually, the condition degrades due to a series of failures or a failure that allows the system to be run improperly for a period of time. However, the time effect could not be evaluated in this analysis and it was assumed that all conditions that could result in damage occurred instantaneously.

The fault trees were developed to the level sufficient to identify primary component failures. Where several component failures resulted in a same system effect, the component failures were grouped together and given a reference number. All primary events contain one or more reference numbers. The individual failure modes included in the reference numbers can be obtained by finding the number in the failure modes and effects analysis summary sheets, which in turn, list the individual failure mode line items. This grouping of failure modes causing the same effects results in simplified fault trees. In many cases, there are 10 to 15 "OR" conditions that would result in the same system effect. The depth of the fault trees is anywhere from 2 to 10 levels. Adding separate primary event circles for each component failure mode would only clutter the already complex fault trees and add nothing to the logic.

D. POINTS OF INTEREST

D.(1) General

The fault trees for all 3 vessels exhibit 2 major types of similarities. These are (1) a larger number of OR-gate relationships than is usually the case with fault trees and (2) many AND-gate relationships characterized by some conditional "input" reflecting, for instance, manual intervention by the crew, the existence of a particular operating mode, etc.. Another type of similarity exists between Ship C (the diesel vessel) and the 2 steam vessels. That is, fairly close parallels exist between speed and direction control faults due to pitch control malfunctions on Ship C and throttle control malfunctions on Ships A and B. In one other area, there are a few points of similarity, namely, the fault tree logic for the 2 steam vessels is somewhat similar in some cases. These areas of similarity are discussed below.

D.(1)(a) AND-Gate/OR-Gate Relationships:

The larger than usual number of OR-gates, and the consequent less than usual number of AND-gates, in all 3 fault trees stems from a basic characteristic of control systems. Since their purpose is to regulate and change, as required, overall system operation, there is no "buffer zone" between the controls and overall system status. In other words, the function of the controls is to "tell" the overall system what to do, and to accomplish this, the controls must have direct access to the system hardware being controlled. This implies that once the controls have generated any particular command, either legitimately or due to malfunction, the command will be acted upon. These resulting actions can range from opening or closing the turbine steam valves to inserting a burner ignitor.

If commands for such actions are generated as a result of a malfunction, they will appear in the fault trees in an AND-gate relationship only if other conditions are required for the action to be carried out. Redundancy is one such condition. In the systems evaluated, only 2 areas of redundancy were found. These were in the control systems' power supplies and in trip circuitry. For power supply malfunctions to cause control system faults, Power Supply #1 and Power Supply #2 must fail. The redundancy in the trip circuitry is implemented to ensure that if a trip condition exists, a trip will occur. Thus, loss of trip capability requires that Trip Circuit #1 and Trip Circuit #2 both fail in such a manner that trip conditions are not recognized. The fault tree AND-gates resulting from these redundancies, however, number fewer than half a dozen.

Another area that can be thought of as redundant exists for all 3 ships. This involves the 2 boilers on both Ships A and B, and the 2 diesel engines on Ship C. Under some conditions, both

boilers or engines must be affected by control system failures to produce an upper level fault tree event. An example of an AND-gate relationship depicting this situation would be independent failures that cause shutdown of both Boiler #1 (or Engine #1) and Boiler/Engine #2. The 3 burners per boiler on Ship A and the 2 burners per boiler on Ship B reflect a similar situation in the fault trees. These boiler-burner-engine AND-relationships constitute very roughly about a third of all fault tree AND-gates.

Very roughly about another third of the fault tree AND-gates represent situations where manual intervention can prevent the fault from "taking effect." These situations involve processes which continue somewhat normally for some finite period after the failure has occurred. If the crew is alerted to such a condition, and takes the proper action, the fault can be avoided. An example would be a failure that shuts down the feedwater supply to a boiler. Following the loss of the feedwater supply, a few minutes would be available to activate a back-up supply if the crew was alerted by a drum-level low alarm and then responded correctly. These situations are depicted in the fault trees as "failure occurs and manual intervention is not effective." Obviously, non-effective manual intervention can be caused by loss of the alerting alarm, failure of the crew to respond to the alarm, or incorrect crew action after responding to the alarm.

The remaining approximately one-third of the fault tree AND-gates reflect some type of conditional requirements. In these situations, both the specific hardware failure and some other condition must exist for the upper level fault to occur. For a potential boiler explosion, for instance, both a fuel source and a combustion source must exist. For a potential boiler overpressure, steam demand must decrease and steam supply must fail to be cut back. Other examples would include failures which effected only certain modes of operation; e.g., loss of speed control in the manuevering mode. (The fault tree would require that this failure occurred and that the vessel was in the maneuvering mode.)

On the 2 steam vessels, there is about a 50-50 ratio of AND to OR gates in the fault trees. On the diesel vessel, the ratio is about 85 percent OR's to 15 percent AND's. This number of OR-gates implies that many failures can "ripple up" to the top of the trees with little to impede them.

D.(1)(b) Diesel/Steam Vessel Similarity:

As indicated above, there are fairly close parallels between speed and direction control faults due to pitch control malfunctions on Ship C and throttle control malfunctions on Ships A and B. This is to be expected since the functions of pitch control and throttle control are essentially identical.

Also, both pitch control and throttle control have "direct access," as discussed above, to the vessel hardware being controlled. (Throttle valves on the turbine vessels and CPP on the diesel vessel.) Many possible control failures will therefore result in incorrect commands to the controlled elements.

D.(1)(c) Similarity Of The Turbine Vessels:

As noted above, there are a few points of similarity in the logic layouts of the fault trees for Ships A and B. Major differences involve the 3 burners per boiler on Ship A vs. 2 burners per boiler on Ship B, the inclusion of automatic burner demand sequencing on Ship A, the provision of more trip features on Ship B, etc.. The individual fault tree probabilities are, of course, different for the 2 ships due to such factors as the use of pneumatics on Ship A, the hardware required for control of the third burner, etc..

The similarity of the fault tree layouts for the 2 vessels exists at the top-most and bottom-most levels and indicates that while the intermediate paths differ, neither system introduces many unique fault events of its own. Since only 2 systems were evaluated, it is not reasonable to conclude that this would be the case for any steam control system. Since the systems evaluated utilized different technological approaches, however, it does not seem likely that other systems would introduce fault tree relationships vastly different from those identified during this study.

D.(2) Quantitative Points Of Interest

D.(2)(a) Ships A and B

A significant point of interest with respect to the steam vessel fault tree quantitative analysis concerns the effect of manual intervention. By computing the probabilities twice, once assuming that manual intervention was never effective, and once assuming that it was effective 90% of the time, considerable overall difference in the numerical results occurred. As discussed in the following section, this manual intervention is primarily possible because of the grace period provided by pipeline processes. At the top level of the fault tree, effective intervention actions can approximately halve the probability of the fault.

Another point of interest concerns boiler explosions. The top level probability of this fault is quite low, in part because of the AND-gates in this logic. A significant number of these AND-gates depict the conditions needed for an explosion, e.g., a fuel source AND an ignition source. Also, while there are a number of potentially critical failure modes in this log-

ic, e.g., purge occurs without airflow, most of the failure mode probabilities are low.

The top level probability of boiler overpressure is also quite low. This chiefly occurs because overpressure conditions are provided with protective trips and shutdowns. For an overpressure fault to occur, both an overpressure condition AND loss of overpressure protection must occur. In general, the probabilities of losing the protection features are quite low.

The probabilities associated with loss of both boilers and turbine shutdown are relatively high. This occurs in part because the fault tree logic for both of these faults involves a large number of OR-gates. Also, there are several failure modes with relatively high probabilities. Both the number of OR-gates and the relatively high probability failure modes results in a number of fault paths with higher probabilities than is generally the case for other fault tree logic.

In the area of turbine damage, a large portion of the failure modes contributing to the top events are provided with protective features. Where trips are provided, an AND situation occurs because the failure mode must occur AND the protective feature must fail to result in turbine damage. Such AND conditions significantly reduce the probability of damage from the their associated failure modes. Where no protection features are provided, the resulting OR situations cause the associated failure mode probabilites to accumulate.

The top level probability for speed/direction control faults is quite low. This occurs because of the AND situation depicting the backup provided by the handpump and turning gear. Without these backup provisions, the top level probability would be significantly higher. Also, a considerable portion of it would be due to failures in the hydraulics.

D.(2)(b) Ship C

The Ship C fault tree is characterized by three major quantitative points of interest. These are:

a) There are very few areas where manual intervention to preclude the failure effect is possible, and numerically, these do not impact the results at all;

b) The individual failure modes have quite low probabilities, with the result that upper level probabilities are also low;

c) The tree logic contains a large proportion of OR-gates, but due to the low individual probabilities this does not lead to relatively high upper level probabilities.

Another point of interest is that all upper level events are very roughly equally likely.

The numerical implications of the Ship C Fault Tree can be summed up as follows: Any fault event is quite roughly just about as likely as any other, although all are relatively unlikely. If a fault event does occur, however, it will generally occur without warning and with no chance of the crew precluding its effect.

IX. CRITICALITY ANALYSIS

A. GENERAL CRITICALITY ASPECTS

During the FMEA and fault tree analyses, it was found that engine room automation systems exhibit 2 classes of system failure effects. The first class can be termed "immediate," since if the specific failure occurs, its effect will occur immediately, without warning, and with no possibility of manual intervention by the crew to prevent or mitigate the failure effect. The second class can be termed "failure effect pending," since there will be some finite period between the time of the failure and the point at which its failure effect is manifested. During this period, it is theoretically possible for the crew to perform some mitigating action so that normal operation is not interrupted.

Failure effects in the immediate class stem from the "direct access" (or, lack of a "buffer zone") of the controls to the elements being controlled, as described in the fault tree discussions in Section VIII.D. Examples of failure effects in this class include trip circuitry failures that cause false trips, and pitch control/turbine control failures that cause uncommanded speed or direction changes.

Defining the criticality of failure effects of the immediate class in qualitative terms is straightforward. If the failure occurs, its effect will occur, so criticality is a function of the failure effect described in the FMEA. These failure effects range from trivial to serious, and the serious ones appear in the fault trees as direct causes or contributing factors to top level fault tree events.

For serious failures of the immediate class, it is impossible to implement alarms that would provide the crew with an advanced warning. However, alarms/indications should be provided to enable the crew to restore normal operations as quickly as possible. Minimizing these failure effects requires reducing the likelihood that the failure occurs.

Failure effects in the "failure effect pending" class involve processes which continue somewhat normally for some finite time period after the failure has occurred. This grace period is exhibited in two situations. The primary one is due to what can be thought of as a pipeline process. An example would be a failure which shuts down the feedwater supply to a boiler. Following the shutdown, some feedwater would remain in the "pipeline" (e.g., in the piping and boiler drum) so that the consequences of the failure would not occur immediately. Another example would involve a failure that caused loss of fuel oil heating. In this case, the failure would cause the fuel oil

to become too viscuous to flow, but some properly heated fuel oil would continue to flow for a few minutes before this occurred.

Since pipeline processes are associated with a number of steam plant control functions, quite a few failure effect pending type failures associated with it were identified for both steam vessels. None were identified for the diesel vessel.

The other situation where failures of the failure effect pending class can occur is associated with provisions for safety shutdowns to preclude machinery damage. This situation requires a failure that causes loss of such shutdown capability and also that a shutdown condition exist (e.g., low lube oil pressure to a turbine or diesel engine, turbine vibration, high diesel jacket water temperature). In these cases, there is some possibility that in the absence of an automatic safety shutdown, the crew might become aware of the situation and initiate a manual shutdown before serious damage had occurred. This is the only type failure of the failure effect pending class identified for the diesel vessel. For both steam vessels, several failures of this type in the turbine controls were identified.

The criticality of the failure effects pending type failures involves several factors. There are, of course, the ultimate consequences if the failure "takes effect." Some of these ultimate consequences are trivial; some are serious. Of equal significance with the ultimate consequence is the length of time of the grace period.

For the failure effects pending type failures identified on the 2 steam vessels, a grace period of about 3 minutes, on average, is available. This figure also appears reasonable for the few failures of this type identified for the diesel vessel.

A period of 3 minutes, more or less, is not sufficient for troubleshooting and repair (except in 1 case---as noted below). It would be sufficient in many cases to go to a manual back-up mode of operation. The lengths of time required for transferring to back-up modes were estimated for Ship A and found also to be applicable to Ship B. These times, which are applicable to a two-man watch, and which could vary plus or minus somewhat, are as follows:

a) 1 minute to 5 minutes maximum to get a boiler back-up under manual control following a boiler shutdown due to automation.

b) 1 minute to 5 minutes maximum to go onto handpump operation following a turbine control problem.

c) 5 minutes to place a remotely located control valve onto manual bypass and manual control.

d) 3 to 5 minutes to restore pump operation under manual control following a pump shutdown caused by automation.

Troubleshooting and repair times are considerably longer. Again, these were estimated for Ship A and found generally applicable to Ship B. They are as follows:

a) Printed circuit card failure:
   1) from 15 minutes to 1 hour if troubleshooting documentation available and card tester utilized.
   2) from 30 minutes to 2 hours if card tester utilized but troubleshooting documentation not available.
   3) indeterminant if card tester not available.

b) Remotely located sensors and valves: from 5 to 30 minutes to troubleshoot; repair time indeterminant, on the order of a half hour to several hours.

c) Relays:
   1) from 15 minutes to 1 hour if troubleshooting documentation available.
   2) indeterminant if troubleshooting documentation not available; in worst case could require a day or more.

d) Set Point Controller (used on Ship A only): 2 minutes to change out the controller; no troubleshooting required, problem obvious by looking at controller. (Note: this is the only case found where repair could be accomplished within the grace period of the pending failure effect).

For the crew to take some mitigating action to a failure effect pending type failure, it must, of course, be alerted and respond to the situation. While a watchstander might be alerted to an abnormal condition by visually monitoring gages and indicators, the alerting function is generally performed by the alarm system.

During this study, it was found that alarm provisions on all 3 vessels appeared to be based on abnormalities due to factors outside the control system. That is, the parameters that were alarmed appeared to be those which could deviate beyond acceptable limits due to problems in the hardware being controlled. For some failure effect pending type failures, the results of control failures are the same as those of non-control failures (e.g., drum level low, steam temperature high, fuel pressure low, etc.).

In other cases, control system failures can produce effects not normally expected in non-control equipment. For instance, a forced draft blower fail alarm is provided on Ship A. In the non-control portion of the combustion air system, loss of air is indeed more likely from fan failure than any other cause. In the control system, however, there is little likelihood of a failure that would shutdown a blower, but there are several failures that would cutback or shutoff the air supply. Such failures would cause a smoke alarm but no alarm specifically indicating a combusiton air problem.

B. QUANTITATIVE CRITICALITY ANALYSIS

Based on the general criticality aspects discussed above, quantitative analyses were conducted to identify and evaluate the interactions, relationships, and ramifications that can impact the severity of a failure. This "severity", in turn, relates to the end effect of the failure on the vessel.

Thus, the quantitative criticality analysis focussed on identifying the various "scenario" factors that determine whether or not a potentially critical failure effect will indeed have critical consequences.

Where these factors and their various ramifications could be quantified, they were included in the quantitative analysis. Other factors and their various ramifications are difficult, and in many cases, impossible to quantify, and they were not quantitatively evaluated.

B.(1) Factors Impacting Criticality

Criticality analyses related to automated propulsion systems are unusually complicated because of the large human factor interface. In addition to the human factors, there are many other factors that can effect the criticality of each failure. Listed below are some that were considered during the criticality analysis. It is emphasized that this entire criticality analysis process is very complicated, and could become a never ending chain of possibilities if all factors were completely analyzed. Therefore, DOVAP selected the primary factors for evaluation since these will generally determine the most likely end effect.

B.(1)(a) Subsystem Effect

The initial criticality consideration involves which subsystem has failed or degraded. This requires that the subsystem be evaluated in terms of its function and relationship to other

subsystems.

B.(1)(b) Component Effect

Component failures within the subsystem have to be evaluated to determine the effect on subsystem criticality. An important part of this evaluation is whether the component is an input or output device. If the component is an input device such as a sensor, usually not only the function fails, but alarms and instruments also fail. If the component is an output device, then using the manual backup mode of operation may not mitigate the effect of the failure. Also, some component failures have relatively little effect on the subsystem performance. An example would be failure of a remote manual function which would only be activated in event of failure of the primary system.

B.(1)(c) Component Failure Mode

A failure mode has a direct bearing on the criticality of the failure. Some failure modes are passive and have little effect on the subsystem performance. The so-called "hardover" failure modes are the most catastrophic to the system, but are often the easiest to detect and isolate. Intermittent failures or marginal failures which create erratic control situations may, in fact, cause more problems than "hardover" failures.

B.(1)(d) Failure Rates

The expected failure frequencies effect criticality. Also, the expected failure frequencies for many components can vary during the vessel's operational life, and this variation must also be considered. Initially failure frequencies will be high due to infant mortality since this type of failure is related to the manufacturing process or installation errors. This period can last anywhere from six months to three years, depending on the types of components and the operational environment. At some point in the operational life, wear-out begins, and this again is dependent on the type of component and will vary with different components. For electronic equipment, the wear-out period has never been established and probably is past the operational life of the equipment. For field equipment, the operational life is probably quite short, and there are some indications that wear-out starts within two or three years of the initial operation of the vessel.

Failure rates are also affected by the amount of functional testing and maintenance, including preventative maintenance and inspection of the equipment. The maintenance philosophy can bring up a whole new series of complex evaluations. The extremes of these philosophies can be to perform no preventative maintenance or inspections, and only perform maintenance as the

equipment fails. The converse would be a detailed maintenance plan with functional testing and checks, scheduled inspections of the equipment, and comprehensive preventative maintenance. In the majority of the cases, the schedule of maintenance for commercial vessels is not pre-planned and is carried out as directed by the chief engineer.

Failure rates also have a direct bearing on the probability of backup equipment being available when needed. If back-up equipment is not periodically checked and maintained, there is no assurance that it will work when required.

Contingency plans for failure conditions also impact criticality and must be based on expected failure rates. Manpower, test equipment, and spares can, depending on their availability, reduce or lengthen the times an equipment is out of service due to failure.

B.(1)(e) Operational Mode

The vessel's mode of operation when a failure occurs is very important to the criticality analysis. Many failures would be highly critical during maneuvering whereas they would have little or no effect during normal cruising. The three phases considered during the criticality analysis were: normal cruising, maneuvering, and light-off.

Normal Cruising

During normal cruising, most temporary failure conditions are not hazardous to the operation of the vessel. There are exceptions to all cases of course, and if the vessel is in close quarters to other vessels or navigation hazards, temporary loss of RPM or direction control would be critical. However, this will not be the case during the majority of the normal cruising time, so these factors were not considered in the criticality analysis.

Maneuvering

Maneuvering is the most critical time period considered in the criticality analysis. Again, in the maneuvering mode, there are many situations where loss of RPM or directional control are not critical. However, a fairly large percentage of the time the vessel will be in close quarters, and the temporary loss of directional or RPM control, or loss of sufficient power for extreme maneuvers would be critical to the vessel.

Light-Off

Again, the criticality of a failure during the light-off phase is determined by the situation at the time. In the criticality analysis, it was assumed that the majority of the

light-offs occur when the throttle is at stop. In some cases, there would be a re-light after maintenance or a boiler trip. These occasions, however, are relatively infrequent and probably occur primarily during normal cruising. Therefore, a problem which causes delays in light-off would usually interfere only with scheduled departure.

B.(1)(f) Watch Size

The number of watchstanders and their background and experience are critical in terms of how quickly normal operation is restored after a failure. Besides the number of watchstanders, the availability of the chief engineer and any other crew members needed to respond to failure situations is also a factor. In the criticality analysis, it was assumed that a two-man watch is maintained at all times and that one of the two is a licensed engineer. The chief engineer is normally in the control room during maneuvering, and would also respond to all alarms and trips. It is estimated that on the average, he would be in the control room within two minutes of any alarm or trip. After observing the operational conditions of selected vessels, it was concluded that, in other than totally unmanned situations, the number of watch personnel during normal cruising is not a criticality-related factor. This is based on the close proximity of the crew's quarters to the control room, and on the generally high reliability of the alarm system. As mentioned above, criticality changes during maneuvering and it is assumed also that the watch size changes and includes the chief engineer.

B.(1)(g) Alarms and Trips

The reliability and coverage of alarms and trips are a very important criticality aspect. For the automated systems evaluated during this study, many failure conditions will activate more than one alarm. As an example, if a failure caused low combustion air, the poor air to fuel ratio would create a smoke condition and a smoke alarm would occur. If the condition continued to degrade until the flame was lost in one burner, a burner management alarm would occur. If this shuts down the boiler, a boiler trip alarm would then occur. If the boiler trip produced a low steam pressure condition, a turbine proportional control malfunction alarm would be activated and the turbine would reduce power. Finally, if the low steam condition continued, a turbine trip and alarm would occur.

In addition to the alarms and trips, the systems evaluated have gauges, read-outs, and lights indicating parameter values and system status. Last but not least, the human interface factor is very important with respect to boiler and turbine conditions and to the implications of alarms and trips. Ever since steam systems have been used for vessel propulsion, the

human senses have played an important role in the safe operation of the systems. The human senses, as well as knowledge of the system, still impact safe system operation. That is, the end determination as to whether a valid alarm condition exists depends on the crew member's appraisal of the situation.

B.(1)(h) Crew Corrective Action

Once it has been determined that a valid alarm exists, the capability of the crew to respond and to take the proper corrective action is a function of their training and experience.

Immediate Response

In the criticality analysis, it was assumed that the immediate crew response would be to restore normal operation as soon as possible. This would be accomplished through the quickest means available to alleviate or by-pass the problem. This could be through use of backup equipment, use of remote/manual capability, or through full manual operation. Another aspect of the immediate response that must be taken into consideration concerns possible equipment damage. For instance, if a high or low water condition exists, the corrective action must be immediate and correct to avoid damage to the boiler or turbine. In many cases during normal cruising, the immediate action will be to prevent equipment damage. On the other hand, during maneuvering or close quarter operations, the immediate action may be to maintain sufficient power or RPM's to avoid a possible collision. Therefore, the training of the crew members in response to certain conditions is a very important part of the criticality analysis.

Troubleshooting and Repair

Troubleshooting and repair is usually conducted after the immediate action has been taken and secured. Troubleshooting and repair may be conducted immediately after the failure occurs or possibly the secondary mode of operation would be continued until the end of the cruise and troubleshooting and/or repair conducted when the vessel reached port. However, the most desirable approach is to restore the system to full automated capabilities as soon as possible. Therefore, the crew members should be capable of troubleshooting and repairing the system.

B.(1)(i) Back-Up Capability

During the criticality evaluation, the back-up modes of operation were considered.

A major consideration associated with the automatic switching of back-up equipment is the reliability of the switching equipment itself. A large amount of the back-up equipment on the vessels evaluated during this study is either in stand-by or is operationally parallel. Most backup pumps and generators are kept on stand-by. That is, they are not in operation until the other pump or generator is taken off line or fails, at which point they are automatically switched in to service. In the case of the boilers, both boilers are operational during normal cruising, and way can be maintained with one boiler at reduced RPM's.

B.(1)(i)(A) Remote Manual Operation of Automated Controls

The remote manual mode of operation is the first back-up selected in case of failure of the primary automated controls. This operational mode can be used if there is a failure in either the input or control logic of the control system.

B.(1)(i)(B) Manual

Boiler front manual control presents several drawbacks. Automatic alarm/trip provisions are disabled in this mode, and the operator must be responsible for monitoring all vital parameters. However, this type of operation has been satisfactory for many decades and if the crew member is properly trained, should provide satisfactory back-up.

B.(1)(j) Troubleshooting Equipment

A factor in the criticality analysis and related to the crew members' capability and training concerns the type of troubleshooting equipment available. This is divided into two major categories: (a) built-in test and (b) individual pieces of test equipment.

B.(1)(j)(A) Built-In Test

Some automated control systems have fairly extensive built-in tests (BIT). Vessel B has a circuit analyzer for the analog section of the controls. This makes it fairly easy to diagnose problems to the circuit card level and then remove and replace the card. However, there is no circuit analyzer for the digital portion of the system, and troubleshooting would be very tedious, if not impossible for the average crew member. Vessels A and C have printed circuit cards with light emitting diode fault indicators. These do not indicate all possible faults however.

B.(1)(j)(B) Test Equipment

Most control system manufacturers provide circuit card testers as optional equipment. These are very important and

should be part of the standard inventory of test equipment on all vessels with automated electronic systems. Card testers should be used to verify that the card removed from the system has indeed failed and that the replacement cards are operational before being installed in the system.

B.(1)(k) Spares

The availability of spares is also a factor in the criticality analysis. If equipment is to be restored to normal operation, adequate spares must be provided. The types of spares carried are a function of crew capability and the type of troubleshooting equipment available. On most vessels, individual piece parts are not replaced on failed cards. However, if a crew member is available with adequate training, and if adequate test equipment is available, the cards could be repaired on board.

B.(1)(l) Technical Documentation

The adequacy of technical documentation is interrelated with test equipment and crew capability in terms of the ability to restore the equipment to normal operation. In evaluating the troubleshooting documentation for the electronic controls on the three vessels considered in this study, it was concluded that sufficient details were not provided for the normal crew member to isolate problems to the failed component. This is especially true for the digital portion of the control systems.

C. QUANTITATIVE CRITICALITY ANALYSIS PROCEDURE

As pointed out, all of the factors above have some bearing on the criticality. In order to evaluate these factors, the following procedures were applied.

C.(1) Grouping of Failure Modes

Failure modes from the FMEA's were grouped whenever possible so that a common criticality analysis could be performed on the group. Each group of failure modes was given a reference number, which is called a criticality number. Each criticality reference number is given in the right-hand column of the individual FMEA sheets and is summarized on the FMEA summary sheets.

C.(2) Criticality Analysis Summary Sheets

For each group of failure modes, a criticality analysis summary sheet was developed. These summaries are presented in

Appendix F. Figure IX-1 is a typical criticality analysis sheet and the following is an explanation of the analysis.

C.(2)(a) Note Number

This is the number that appears in the right-hand column of the FMEA sheets and is the reference note number in the summary sheets. This is also the number corresponding to the lowest level component faults in the fault trees.

C.(2)(b) Failure Effect

The failure effect is the description of the group of failure modes which have been accumulated under one criticality evaluation number.

C.(2)(c) System Effect

This is the most likely effect of the failure on the propulsion system or turbine system. In some cases, there are one or more effects and the effects are given with the most likely being the first.

C(2)(d) Symptom or How Detected

This gives the most likely way that the problem can be detected, and could be an alarm, or trip, or other indications. In many cases, there are multiple ways in which the problem can be detected. In some cases, there are no detection means except that the vessel responds incorrectly.

C(2)(e) Most Likely Action and System Status

This part of the criticality analysis is the most subjective because of the factors listed above, and the many assumptions. To reiterate some of the assumptions previously given:

a) It is assumed that the number of watchstanders during normal cruising does not appreciatively affect the actions taken.

b) The chief engineer is in the control room during maneuvering and light-off.

c) The chief engineer can normally reach the control room within two minutes.

d) In most cases, the watchstander has sufficient time to cross check indicators, lights, and other symptoms, and then takes the proper action.

SHIP B NOTE #24

FAILURE EFFECT: Deaerator high level.

SYSTEM EFFECT: No effect.

SYMPTOM OR HOW DETECTED: Vital alarm in engine room control console. Level transmitter set at 81" (high). Relief valve opens.

MOST LIKELY ACTION AND SYSTEM STATUS

-IMMEDIATE: Verify alarm and check indicators in control console. If cannot clear alarm activate remote manual or manual control.

-SECONDARY ACTION: Troubleshoot system using analog test station. If problem in the field, isolate to component using meters and visual inspection. Replace defective component and return to automatic control.

CRITICALITY EVALUATION:
System Effects:
(a) Normal Steaming: 2 - No effect.
(b) Maneuvering: 32 - No effect.
(c) Light-Off: 61 - Not applicable during this phase.

Mission Effects:
(a) Normal Steaming: 2 - No effect.
(b) Maneuvering: 2 - No effect.
(c) Light-Off: 21 Not applicable during light-off.

FAILURE RATE:
-Transducers = 6.63
-Valves = 49.14
-Electronics = 9.8930
Total = 65.6630

FIGURE IX-1

Typical Criticality Sheet

C.(2)(f) Most Likely Action for Alarm Situation

The most likely action for an alarm situation would be to alleviate the condition that caused the alarm. In most cases, the watchstander would switch the control mode to remote manual and try to restore operation within acceptable limits. If this can be done, operation would probably be continued in this mode until there was sufficient time to troubleshoot and correct the problem. If the remote manual mode did not effectively alleviate the situation, the next action would be to go directly to the field and manually operate the subsystem. Again, when time permitted, troubleshooting and repair could be performed to restore normal automatic control.

C.(2)(g) Boiler Trip

For a boiler trip situation, the immediate action would be to determine the cause of the trip and then alleviate any conditions that would cause boiler or turbine damage. Again, in most cases the watchstander would switch to remote manual, and if this did not rectify the situation, go to the field to correct the problem. Once the cause for the boiler trip had been determined and a back-up system was functioning satisfactorily, the boiler could be re-lit if it was safe to do so. Troubleshooting and restoration to normal automatic operation could then be carried out when time permitted.

C.(2)(h) Turbine Trip

In the case of a turbine trip, the watchstander would immediately go to the handpump mode of operation. For critical situations, many trips can be overridden, again depending on the situation at the time, but the most likely action is to resort to the handpump. Again, troubleshooting and restoration of the system to normal automatic operation could be carried out when time permitted.

C.(3) Systems Effects Summary

For each phase (i.e., light-off, maneuvering, and cruising), a list of systems effects was generated. There are 18 of these, as follows:

1 - Not applicable to this phase: This indicates the failures in the group are not applicable to the particular phase under consideration. (For instance, failures grouped together as causing low steam pressure are not applicable to the light-off phase.)

2 - No effect: This indicates that the failures in the group do not have any effect on the system. (For example, failures of instruments not used

functionally in the system.)

3 - Alarm, activate remote manual: The failures in this group activate an alarm, and the most likely action would be to switch to remote manual means of operation.

4 - Boiler trip, troubleshoot and restart boiler: The boiler cannot be restarted until the problem causing the trip is resolved. Therefore, troubleshooting would be required to determine and correct the reason for trip, then the boiler would have to be restarted.

5 - Auto back-up, back-up takes over function: This is the case, such as with the lube pump, where back-up is automatically switched-in to take over the function if the primary unit fails.

6 - Explosive condition, actual probability of explosion depends on other factors: This condition identifies the group of failures that could be contributing factors to an explosion. However, other factors are usually required for an actual explosion and some of these factors are not a part of the controls system.

7 - Turbine trip, troubleshoot and restart turbine: In most cases, the turbine trips are to protect the turbine from damage. Therefore, the condition must be resolved before the turbine is restarted. However, during critical maneuvering situations, most of the trips can be overridden.

8 - Turbine MPC reduces RPM, troubleshoot and resume normal RPM's: The reduced RPM's can be due to boiler problems or turbine problems. Because the reduced RPM's are instituted to prevent turbine damage and other system complications, the reason for the RPM reduction must be isolated and resolved before normal RPM's can be restored.

9 - False boiler trip, troubleshoot and restart boiler: The false boiler trip must be verified first to ascertain that there is not a bonafide problem; the boiler can then be restarted.

10 - False turbine trip, troubleshoot and restart turbine: Again, on a false turbine trip the cause for the trip must be verified to ascertain that there is not a problem before the turbine is restarted.

11 - No alarm, only lights or indicators show problem

condition: For a few conditions, there are no alarms and the watchstander must observe indicators or lights to detect a problem condition. For an unmanned system, the likelihood of such problems should be carefully evaluated. In the summary section of this report, these will be further commented upon.

12 - Loss of back-up or alarm: In the criticality analysis, it is assumed that the most likely action is for back-up equipment to take over the function, or for alarms to alert the crew to activate the secondary controls. However, some groups of failure modes result in the loss of these back-up capabilities.

13 - False alarm: False alarms are a constant problem, especially during initial operation of a system and are time-consuming. However, they have no effect on mission criticality.

14 - Loss of trip: Loss of trip functions could result in major equipment damage. In most cases, the loss must also be accompanied by loss of the associated alarm.

15 - Light-off inhibited or aborted: Many failure conditions in the burner or combustion logic will inhibit the automatic burner light-off process. However, the burner light-off process is a convenience and manual light-off will usually rectify the condition.

16 - Erratic RPM's, turbine control failure, activate handpump: Many failure conditions in the throttle control result in erratic or loss of control over RPM's. In the majority of the cases, the handpump would be activated and remain in use until the problem had been resolved.

17 - Erratic directional control, turbine control failure, activate handpump: Many of the failure groups for the throttle control result in loss of directional control. In these cases, the handpump would be activated and remain in use until the problem has been isolated and corrected.

18 - Loss of protective feature: This involves the loss of protective features other than trips and can result in damage to the equipment it is associated with.

C.(4) Mission Criticality

The mission criticality for the three phases of operation was grouped into common end effects. There are twelve groups for normal steaming and maneuvering, and six groups for light-off. For each type of end effect, a criticality factor was assigned. This factor ranges from 0 to 1, with 0 being no effect and 1 being extreme criticality or total mission loss. The mission criticality factor again is based on most likely situations, and varies with the mission phases. Temporary performance degradation during normal steaming has a minor effect upon criticality, whereas during maneuvering, it could be disastrous. During light-off, it is assumed that the majority of light-offs occur while docked and delays in light-off are not critical to the vessel operation. End effect groupings for normal steaming and maneuvering are as follows:

a) Not applicable during normal steaming: This group of failures relate to other phases, for instance, they would inhibit light-off, etc., and would not be applicable to normal steaming.
Normal Steaming: P = 0.0
Maneuvering: P = 0.0

b) No effect: This is the same as the no effect group in the system level coding, and as an example again, instrument failures would have no effect on the vessel end effects.
Normal Steaming: P = 0.0
Maneuvering: P = 0.0

c) Slight performance degradation: This group covers failures where an alarm sounds and the situation can be rectified by resorting to remote manual operation. In the remote manual, system response will not be as instantaneous as in the automatic mode, and this will result in a slight performance degradation.
Normal Steaming: P = 0.1
Maneuvering: P = 0.6

d) Temporarily reduced RPM: Failures in this group cause a boiler trip or reduced RPM due to action of the turbine MPC controls. During normal steaming, reduced RPM's are of minor criticality and full RPM can be restored in a relatively short time. During maneuvering, reduced RPM's could be critical, therefore, criticality is significantly higher during the maneuvering phase.
Normal Steaming: P = 0.4
Maneuvering: P = 0.7

e) Possible turbine damage: Turbine damage can result from loss of turbine protective features. Damage usually is not instantaneous but rather the result of many cumulative overstresses. The possibility is difficult to evaluate quantitatively; however, if it should occur, partial or total loss of the propulsion system could result.
Normal Steaming: P = 0.5
Maneuvering: P = 0.5

f) Possible boiler damage: Boiler damage can result from control failures or a combination of control and external failures. Damage can also result from either accumulated effects over some period or instantaneously, such as from an explosion. Again, the quantitative probability of damage is difficult to evaluate; however, if damage does occur, the possibility of total loss of the boiler is very high and therefore, the criticality value must reflect this possibility.
Normal Steaming: P = 0.5
Maneuvering: P = 0.5

g) Large performance degradation: Failure modes in this group necessitate total manual operations. This could be operation of a control valve by hand in the field, complete manual operation of a boiler, or use of the handwheels for turbine control. This results in slow response and inefficient operations. There is also a large chance of human error in this type of operation because in some cases, the control valves are widely separated and communications could be a factor.
Normal Steaming: P = 0.6
Maneuvering: P = 0.8

h) Temporarily dead in water: In this group of failures, the turbine will trip but the problem can be rectified in a relatively short period of time. Again, during normal steaming, this is not a critical situation; however, in maneuvering, it is very serious.
Normal Steaming: P = 0.7
Maneuvering: P = 0.9

i) Dead in water: Failures in this group cause loss of propulsion, and the situation will be such that corrective actions require lengthy time periods. This is a remote possibility and is a worst case

situation.
Normal Steaming: P = 0.9
Maneuvering: P = 1.0

j) Temporary loss of RPM control: This group covers turbine control malfunctions requiring use of the handpump back-up until control is restored. Handpump control results in slow RPM response for large changes; however, for normal cruising, this is not critical.
Normal Steaming: P = 0.6
Maneuvering: P = 0.9

k) Temporary loss of directional control: Failures in this group cause loss of directional control, requiring that the handpump be utilized. This is not critical during normal steaming; however, slower directional response during maneuvering is highly critical.
Normal Steaming: P = 0.6
Maneuvering: P = 0.9

l) Back-up failure, primary and back-up must both fail: The FMEA's and criticality analysis are based on single failures; multiple failures are considered in the fault tree analysis. However, in order to allow for the possibility of multiple failures, they must be covered in the mission criticality analysis.
Normal Steaming: P = 0.2
Maneuvering: P = 0.4

End effect mission criticality groupings for the light-off phase are as follows:

21 - Not applicable during light-off: Failures in this group do not apply to the lightoff phase.
P = 0.0

22 - No effect: Failures in this group have no effect during the light-off phase.
P = 0.0

23 - Slight delay in light-off: A slight delay in light-off can occur when a problem must be alleviated by going to remote manual before automatic light-off can proceed.
P = 0.2

24 - Delay in light-off: Delay in light-off occurs when extensive troubleshooting must be performed

before light-off can commence, or when light-off must be performed manually at the boiler front.
P = 0.4

25 - Possible boiler damage: Possible boiler damage can occur because of explosive conditions during light-off, such as inadequate or loss of purge. Also, possible damage can occur because of loss of fire during light-off. In most cases, possible boiler damage is a multiple failure situation and factors outside of the control system influence the possibility.
P = 0.5

26 - Possible turbine damage: Possible turbine damage can occur when light-off is initiated during normal cruising.
P = 0.5

C.(5) Quantitative Criticality Computer Analysis

A computer analysis was performed on the criticality data developed for Ship B. Ship B was selected because it is a typical system and the distribution of mission effect for Ship A would be similar except that failure occurrences would possibly be more frequent. Ship C was not analyzed because the criticality associated with diesel systems is fairly straightforward. The computer software utilized for this evaluation was developed by Management Sciences, Inc. and is entitled Systems Evaluation Analysis (SEA). The SEA output lists system effects and mission effects in rank order according to their contribution to mission criticality.

C.(5)(a) Input Data

Data for three operational phases (normal cruising, maneuvering, and light-off) was inputted. The time used for normal cruising was 710 hours, for maneuvering 20 hours, and for the burner management logic 730 hours. The rationale for these times is that, on average, a typical complete round-trip is approximately one month or 730 hours. Approximately 20 hours are spent maneuvering, which leaves the remaining 710 hours for cruising. The third phase, light-off, is primarily associated with the burner management logic which is constantly on, and therefore the operating hours are the total 730 hours. Four factors were entered for modifying the basic failure rates. These are (1) temperature factors for increasing the ambient temperature from 35^{o} C. to 50^{o} C., (2) quality factors for changing from commercial level parts to military grade parts,

(3) premature failure factors for converting steady state failure rates to premature failure rates, and (4) a maintenance factor which reflects the reduction in failure rates that can be expected through a detailed inspection, test, and preventative maintenance plan.

Tables of mission effects and system effects for the three phases were entered into the data base. The software is structured to evaluate groups of equipment. In this analysis, each group is a subsystem. Each group is subdivided into functions and each function is a different part class. Part classes consist of electronic parts, transducers, sensors, valves, and similar breakdowns. For each function, the basic failure rate is given, as is the quantity of subsystems per vessel, and the four factors. The failure modes for each function are given immediately following the function. Each failure mode contains a code which is the criticality reference number. Each mode also has the applicable system failure effect for the three phases and the percent that the failure mode contributes to the function failure rate. A brief narrative explanation of the mode is also given.

C.(5)(b) Computer Output

The software analyzes one phase at a time. For each mode which was inputted, the probability of the mode occurring is computed for the selected phase, along with the associated mission criticality. Also given for each mode is the system effect. These modes are grouped as inputted, that is, by subsystem and function.

Following the mode effects are the system effects criticality summary by groups. This summary compares the various system effects for a particular subsystem against the total for the entire control system. The probability of each system effect is given, as is the percent contribution for the subsystem being analyzed and for the total system. The system criticality is also computed for each system effect, and the percent contribution to the subsystem is calculated along with the percent for the total system. Following the group analysis is the overall system effects summary, giving all system effects ranked by contribution to the overall criticality.

The next section is the mission effects for the total system again ranked by contribution to the total system criticality. Following this are the mission effect summaries, giving the contribution of each mission effect by subsystems. The mission and system summaries are presented in Figures IX-2 through IX-6. Examples of the input data are given in Figure IX-7. The detailed printouts are presented in Appendix G.

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY	MISSION LOSS PROB.	SYSTEM CRITICALITY	PERCENT OF CONTRIBUTION ALL GROUPS CRITICALITY
33	ALARM/ACTIVATE REMOTE MANUAL	33	.1359E-01	24.5375	0.6000	.8153E-02	37.9182
34	RLR TRIP/CORRECT/RESTART RLR	35	.5667E-02	10.2304	0.7000	.3966E-02	18.4461
41	NO ALARM--ONLY LIGHT/INDICATOR	37	.3656E-02	6.5990	0.5000	.1827E-02	8.4975
42	AUTO CONTROL OUTPUT IS ERRATIC	33	.3036E-02	5.4799	0.6000	.1821E-02	8.4686
38	HPC REDUCES RPM/CORRECT/RESUME	35	.2084E-02	3.7618	0.7000	.1458E-02	6.7834
46	LOSS OF TRIP	37	.2859E-02	5.1600	0.5000	.1428E-02	6.6440
36	EXPLOSIVE CONDITION	37	.2345E-02	8.2323	0.5000	.1172E-02	5.4519
43	LOSS OF BACK-UP OR ALARM	44	.2649E-02	4.7813	0.4000	.1059E-02	4.9266
37	TURB TRIP--CORRECT/RESTART BLR	40	.4929E-03	0.8897	0.9000	.4436E-03	2.0631
50	LOSS OF PROTECTIVE FEATURE	37	.2389E-03	0.4312	0.5000	.1194E-03	0.5554
48	FALSE TURB TRP/CORRECT/RESTART	48	.3311E-04	0.0598	0.9000	.2980E-04	0.1386
64	RLR TRIP/CORRECT/RESTART RLR	23	.1150E-03	0.2076	0.2000	.2300E-04	0.1070
14	FALSE ALARM	2	.2443E-03	0.4410	0.0	.0	0.0
31	NOT APPLICABLE TO THIS PHASE	31	.1226E-01	22.1321	0.0	.0	0.0
32	NO EFFECT	32	.3232E-02	5.8335	0.0	.0	0.0
35	AUTO BACK-UP TAKES OVER	32	.2423E-02	0.3734	0.0	.0	0.0
44	FALSE ALARM	32	.4707E-03	0.8496	0.0	.0	0.0

FIGURE IX-2

System Criticality for Maneuvering
(20 Hours per Cruise)

MISSION EFFECT CRITICALITY

MISSION EFFECT	NO.	SYSTEM EFFECT FAILURE PROBABILITY	PCT. OF SYSTEM FAILURE PROBABILITY	MISSION LOSS PROBABILITY	MISSION CRITICALITY	PERCENT CONTRIBUTION TO MISSION CRITICALITY
33 SMALL PERFORMANCE DEGRADATION	1	.1663E-01	30.02	.6000	.9973E-02	46.39
35 TEMPORARY REDUCED RPMS	2	.7751E-02	13.99	.7000	.5424E-02	25.23
37 POSSIBLE RLR/TURB DAMAGE	3	.9098E-02	16.42	.5000	.4547E-02	21.15
48 BACK-UP FAILURE	4	.2649E-02	4.781	.4000	.1059E-02	4.927
49 TEMPORARY DIM	5	.5260E-03	.9495	.9000	.4734E-03	2.202
23 SLIGHT DELAY IN LIGHT-OFF	6	.1150E-03	.2076	.2000	.2300E-04	.1070
31 NOT APPLICABLE/MANEUVERING	31	.1226E-01	22.13	.0	.0	.0
32 NO EFFECT	32	.6125E-02	11.06	.0	.0	.0
2 NO EFFECT	35	.2443E-03	.4410	.0	.0	.0

FIGURE IX-3

Mission Criticality for Maneuvering
(20 Hours per Cruise)

SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY	MISSION LOSS PROB.	SYSTEM CRITICALITY	PERCENT OF CONTRIBUTION ALL GROUPS CRITICALITY
77 LIGHT-OFF INHIBITS OR ABORTED	28	.6306	31.1888	0.4000	.2490	32.5264
66 EXPLOSIVE CONDITION	29	.1919	9.4930	0.5000	.9806E-01	12.8080
76 LOSS OF TRIP.	25	.1043	5.1600	0.5000	.5113E-01	10.7869
73 LOSS OF BACK-UP OR ALARM	24	.9668E-01	4.7813	0.4000	.3834E-01	8.0276
72 AUTO CONTROL OUTPUT IS ERRATIC	23	.9703E-01	4.7988	0.2000	.1915E-01	4.0065
34 BLR TRIP/CORRECT/RESTART BLR	35	.1866E-01	0.9228	0.7000	.1300E-01	2.7269
74 FALSE ALARM	23	.3039E-01	1.5029	0.2000	.6053E-02	1.2673
63 ALARM/ACTIVATE REMOTE MANUAL	24	.1025E-01	0.5072	0.4000	.4091E-02	0.8566
67 TURB TRIP--CORRECT/RESTART BLR	23	.1025E-01	0.5072	0.2000	.2046E-02	0.4283
61 NOT APPLICABLE TO THIS PHASE	21	.8042	39.7720	0.0	.0	0.0
62 NO EFFECT	22	.5826E-02	0.2882	0.0	.0	0.0
65 AUTO BACK-UP TAKES OVER	22	.2178E-01	1.0771	0.0	.0	0.0

FIGURE IX-4

System Criticality for Light-Off
(Burner Management always on, 730 hours per cruise)

MISSION EFFECT CRITICALITY

MISSION EFFECT	NO.	SYSTEM EFFECT FAILURE PROBABILITY	PCT. OF SYSTEM FAILURE PROBABILITY	MISSION LOSS PROBABILITY	MISSION CRITICALITY	PERCENT CONTRIBUTION TO MISSION CRITICALITY
24 DELAY IN LIGHT-OFF	1	.7376	36.48	.4000	.2914	61.01
25 POSSIBLE BOILER DAMAGE	2	.2963	14.65	.5000	.1460	30.56
23 SLIGHT DELAY IN LIGHT-OFF	3	.1377	6.809	.2000	.2724E-01	5.704
35 TEMPONARY REDUCED RPMS	4	.1866E-01	.9228	.7000	.1300E-01	2.721
21 NOT APPLICABLE/LIGHT-OFF	21	.8042	39.77	.0	.0	.0
22 NO EFFECT	22	.2761E-01	1.365	.0	.0	.0

FIGURE IX-5

Mission Criticality for Light-Off
(Burner Management always on, 730 hours per cruise)

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY	MISSION LOSS PROB.	SYSTEM CRITICALITY	PERCENT OF CONTRIBUTION ALL GROUPS CRITICALITY
4	BLR TRIP/CORRECT/RESTART BLR	5	.2273	11.5598	0.4000	.9082E-01	24.6568
11	NO ALARM--ONLY LIGHT/INDICATOR	7	.1298	6.5990	0.5000	.6383E-01	17.4025
16	LOSS OF TRIP	7	.1015	5.1600	0.5000	.4975E-01	13.6277
3	ALARM/ACTIVATE REMOTE MANUAL	3	.4956	25.2022	0.1000	.4884E-01	13.3835
6	EXPLOSIVE CONDITION	7	.8323E-01	4.2323	0.5000	.4136E-01	11.3279
8	MPC REDUCES RPM/CORRECT/RESUME	5	.6228E-01	3.1669	0.4000	.2472E-01	6.7705
13	LOSS OF BACK-UP OR ALARM	14	.9403E-01	4.7813	0.2000	.1865E-01	5.1088
7	TURB TRIP--CORRECT/RESTART BLR	10	.1750E-01	0.8897	0.7000	.1222E-01	3.3461
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.1078	5.4798	0.1000	.1064E-01	2.9155
20	LOSS OF PROTECTIVE FEATURE	7	.8489E-02	0.4312	0.5000	.4222E-02	1.1564
10	FALSE TURB TRP/CORRECT/RESTART	10	.1175E-02	0.0598	0.7000	.8223E-03	0.2252
5	AUTO BACK-UP TAKES OVER	2	.8601E-01	4.3734	0.0	.0	0.0
14	FALSE ALARM	2	.2956E-01	1.5029	0.0	.0	0.0
1	NOT APPLICABLE TO THIS PHASE	1	.4076	20.7281	0.0	.0	0.0
2	NO EFFECT	2	.1147	5.8335	0.0	.0	0.0

FIGURE IX-6

System Criticality for Normal Steaming
(710 hours per cruise)

MISSION EFFECT CRITICALITY

MISSION EFFECT	NO.	SYSTEM EFFECT FAILURE PROBABILITY	PCT. OF SYSTEM FAILURE PROBABILITY	MISSION LOSS PROBABILITY	MISSION CRITICALITY	PERCENT CONTRIBUTION TO MISSION CRITICALITY
7 POSSIBLE BLR/TURB DAMAGE	1	.3230	16.42	.5000	.1592	43.59
5 TEMPORARY REDUCED RPMS	2	.2896	14.73	.4000	.1147	31.83
3 SMALL PERFORMANCE DEGRADATION	3	.6034	30.68	.1000	.5951E-01	16.30
14 BACK-UP FAILURE	4	.9403E-01	4.781	.2000	.1865E-01	5.108
10 TEMPORARY DIM	5	.1867E-01	.9495	.7000	.1304E-01	3.571
1 NOT APPLICABLE/NORMAL STEAMING	7	.4076	20.73	.0	.0	.0
2 NO EFFECT	10	.2303	11.71	.0	.0	.0

FIGURE IX-6A

Mission Criticality for Normal Steaming
(710 Hours per Cruise)

FIGURE IX-7

Input Data for Computer Criticality Analysis
Ship B

```
PREDICTOR 8.0 217c Notice=1

Run on 09/07/82 at 12.27.45

READY;
OFFLINE READ CRIT ANAL
SET WIDE ON
SET 217C ON
SET NOTICE 1 ON
SET ENV NS
SET T 35
SET PHASE TIMES 710 20 730
SET CRITICALITY ON
SET IGNORE SFACTOR
SET IGNORE RFACTOR
SET IGNORE SF
SET IGNORE RF
SET SELECT PHASE 1
SET MFE=1 P=0.0 NOT APPLICABLE/NORMAL STEAMING
SET MFE=2 P=0.0 NO EFFECT
SET MFE=3 P=0.1 SMALL PERFORMANCE DEGRADATION
SET MFE=5 P=0.4 TEMPORARY REDUCED RPM'S
SET MFE=7 P=0.5 POSSIBLE BLR/TURB DAMAGE
SET MFE=9 P=0.6 LARGE PERFORMANCE DEGRADATION
SET MFE=10 P=0.7 TEMPORARY DIM
SET MFE=11 P=0.9 DIM
SET MFE=12 P=0.6 TEMPORARY LOSS OF RPM CONTROL
SET MFE=13 P=0.8 TEMP LOSS DIRECTIONAL CONTROL
SET MFE=14 P=0.2 BACKUP FAILURE
SET MFE=31 P=0.0 NOT APPLICABLE/MANEUVERING
SET MFE=32 P=0.0 NO EFFECT
SET MFE=33 P=0.6 SMALL PERFORMANCE DEGRADATION
SET MFE=35 P=0.7 TEMPORARY REDUCED RPM'S
SET MFE=37 P=0.5 POSSIBLE BLR/TURB DAMAGE
SET MFE=39 P=0.8 LARGE PERFORMANCE DEGRADATION
SET MFE=40 P=0.9 TEMPORARY DIM
SET MFE=41 P=1.0 DIM
SET MFE=42 P=0.9 TEMPORARY LOSS OF RPM CONTROL
SET MFE=43 P=0.9 TEMP LOSS DIRECTIONAL CONTROL
SET MFE=44 P=0.4 BACKUP FAILURE
SET MFE=45 P=0.0 NOT APPLICABLE/MANEUVER
```

FIGURE IX-7 (cont)

```
SET MFE=22 P=0.0 NO EFFECT
SET MFE=23 P=0.2 SLIGHT DELAY IN LIGHT-OFF
SET MFE=24 P=0.4 DELAY IN LIGHT-OFF
SET MFE=25 P=0.5 POSSIBLE BOILER DAMAGE
SET SFE=1, MFE=1 NOT APPLICABLE TO THIS PHASE
SET SFE=2, MFE=2 NO EFFECT
SET SFE=3, MFE=3 ALARM/ACTIVATE REMOTE MANUAL
SET SFE=4, MFE=5 BLR TRIP/CORRECT/RESTART BLR
SET SFE=5, MFE=2 AUTO BACK-UP TAKES OVER
SET SFE=6, MFE=7 EXPLOSIVE CONDITION
SET SFE=7, MFE=10 TURB TRIP--CORRECT/RESTART TURB
SET SFE=8, MFE=5 MPC REDUCES RPM/CORRECT/RESUME
SET SFE=9, MFE=5 FALSE BLR TRIP/CORRECT/RESTART
SET SFE=10 MFE=10 FALSE TURB TRP/CORRECT/RESTART
SET SFE=11, MFE=7 NO ALARM--ONLY LIGHT/INDICATOR
SET SFE=12, MFE=3 AUTO CONTROL OUTPUT IS ERRATIC
SET SFE=13, MFE=14 LOSS OF BACK-UP OR ALARM
SET SFE=14, MFE=2 FALSE ALARM
SET SFE=15, MFE=7 LOSS OF TRIP
SET SFE=17, MFE=1 LIGHT-OFF INHIBITS OR ABORTED
SET SFE=18, MFE=12 ERRATIC RPM'S/USE HANDPUMP
SET SFE=19, MFE=13 ERRATIC DIR CONTROL/USE HDPMP
SET SFE=20, MFE=7 LOSS OF PROTECTIVE FEATURE
SET SFE=31, MFE=31 NOT APPLICABLE TO THIS PHASE
SET SFE=32, MFE=32 NO EFFECT
SET SFE=33, MFE=33 ALARM/ACTIVATE REMOTE MANUAL
SET SFE=34, MFE=35 BLR TRIP/CORRECT/RESTART BLR
SET SFE=35, MFE=32 AUTO BACK-UP TAKES OVER
SET SFE=36, MFE=37 EXPLOSIVE CONDITION
SET SFE=37, MFE=40 TURB TRIP--CORRECT/RESTART TURB
SET SFE=38, MFE=35 MPC REDUCES RPM/CORRECT/RESUME
SET SFE=39, MFE=35 FALSE BLR TRP/CORRECT/RESTART
SET SFE=40, MFE=40 FALSE TURB TRP/CORRECT/RESTART
SET SFE=41, MFE=37 NO ALARM--ONLY LIGHT/INDICATOR
SET SFE=42, MFE=33 AUTO CONTROL OUTPUT IS ERRATIC
SET SFE=43, MFE=44 LOSS OF BACK-UP OR ALARM
SET SFE=44, MFE=32 FALSE ALARM
SET SFE=45, MFE=37 LOSS OF TRIP
SET SFE=47, MFE=31 LIGHT-OFF INHIBITS OR ABORTED
SET SFE=48, MFE=42 ERRATIC RPM'S/USE HANDPUMP
SET SFE=49, MFE=43 ERRATIC DIR CONTROL/USE HDPMP
SET SFE=50, MFE=37 LOSS OF PROTECTIVE FEATURE
SET SFE=61, MFE=21 NOT APPLICABLE TO THIS PHASE
SET SFE=62, MFE=22 NO EFFECT
SET SFE=63, MFE=24 ALARM/ACTIVATE REMOTE MANUAL
SET SFE=64, MFE=23 BLR TRIP/CORRECT/RESTART BLR
SET SFE=65, MFE=22 AUTO BACK-UP TAKES OVER
SET SFE=66, MFE=25 EXPLOSIVE CONDITION
SET SFE=67, MFE=23 TURB TRIP--CORRECT/RESTART TURB
SET SFE=72, MFE=23 AUTO CONTROL OUTPUT IS ERRATIC
SET SFE=73, MFE=24 LOSS OF BACK-UP OR ALARM
SET SFE=74, MFE=23 FALSE ALARM
SET SFE=76, MFE=25 LOSS OF TRIP
SET SFE=77, MFE=23 LIGHT-OFF INHIBITS OR ABORTED
SET SFE=77, MFE=24 LIGHT-OFF INHIBITS OR ABORTED
SET SFE=80, MFE=25 LOSS OF PROTECTIVE FEATURE
SET GROUP 1 NAME=BURNER MANAGEMENT/MASTER
SET GROUP 2 NAME=BURNER MODULE
SET GROUP 3 NAME=COMBUST CNTL/ALR 2ND LGC
SET GROUP 4 NAME=COMBUSTION CONTROL
SET GROUP 5 NAME=DRUM LEVEL CONTROL
SET GROUP 6 NAME=FEEDWATER CONTROL
SET GROUP 7 NAME=FW RECRC VALVE CONTROL
SET GROUP 8 NAME=SHTR STM TEMP CNTL
SET GROUP 9 NAME=STEAM DUMP CONTROL
SET GROUP 10 NAME=FWD PR START/STOP CNTL MODULE
```

FIGURE IX-7 (cont)

```
SET GROUP 11 NAME=DEAERATOR LEVEL CONTROL
SET GROUP 12 NAME=FUEL OIL HEADER TEMP
SET GROUP 13 NAME=FO RECRC CONTROL
SET GROUP 14 NAME=LO PUMP CONTROLS
SET GROUP 15 NAME=ITC
SET BLOCK 1 NAME=RUNNER MANAGEMENT/MASTER
SET BLOCK 2 NAME=RUNNER MODULE
SET BLOCK 3 NAME=COMBUST CNTL/PLP DMD LOG
SET BLOCK 4 NAME=COMBUSTION CONTROL
SET BLOCK 5 NAME=DRUM LEVEL CONTROL
SET BLOCK 6 NAME=FEEDWATER CONTROL
SET BLOCK 7 NAME=FW RECRC VALVE CONTROL
SET BLOCK 8 NAME=SHTR STM TEMP CNTL
SET BLOCK 9 NAME=STEAM PUMP CONTROL
SET BLOCK 10 NAME=F-D FD START/STOP CNTL MODULE
SET BLOCK 11 NAME=DEAERATOR LEVEL CONTROL
SET BLOCK 12 NAME=FUEL OIL HEADER TEMP
SET BLOCK 13 NAME=FO RECRC CONTROL
SET BLOCK 14 NAME=LO PUMP CONTROLS
SET BLOCK 15 NAME=ITC
SET GROUP 1 ON
SET BLOCK 1 ON
SET FUNCTION ELECTRONIC/RNR MGT MST
PARTS FR=0.0001 QTY=2 RFACTOR=1.12 RF=0.22 SFACTOR=3.25 SF=0.80
SET MODE=1 CODE=1 SFE=1,31,77 P=.090 MODE=LOSS OF PURGE
SET MODE=2 CODE=2 SFE=1,31,77 P=.007 MODE=INADVERTENT PURGE
SET MODE=3 CODE=3 SFE=1,31,77 P=.227 MODE=FLIGHT-OFF LOGIC FAILURE
SET MODE=4 CODE=4 SFE=1,31,77 P=.373 MODE=LOSS OF TRIP
SET MODE=5 CODE=5 SFE=1,31,77 P=.004 MODE=INADVERTENT PURGE
SET MODE=6 CODE=6 SFE=1,31,77 P=.040 MODE=LOSS/INADEQUATE RECRC
SET MODE=7 CODE=7 SFE=1,31,77 P=.113 MODE=FALSE TRIP
SET MODE=8 CODE=127 SFE=4,34,77 P=.124 MODE=FOTV CLOSES OR CAN'T OPEN
SET MODE=9 CODE=1271 SFE=4,34,77 P=.124 MODE=FOTV CLOSES OR CAN'T OPEN
SET MODE=10 CODE=128 SFE=1,31,66 P=.017 MODE=FOTV OPEN OR CAN'T CLOSE
SET MODE=11 CODE=1281 SFE=1,31,66 P=.017 MODE=FOTV OPEN OR CAN'T CLOSE
SET MODE=12 CODE=1282 SFE=1,31,66 P=.017 MODE=FOTV OPEN OR CAN'T CLOSE
SET MODE=13 CODE=131 SFE=10,46,76 P=.024 MODE=LOSS OF BOILER TRIP
SET MODE=14 CODE=132 SFE=1,31,66 P=.039 MODE=LOSS OF PURGE TIMER
SET MODE=15 CODE=134 SFE=1,31,66 P=.003 MODE=PURGE INTITIATED/NO INHBT
SET MODE=16 CODE=135 SFE=1,31,66 P=.013 MODE=AIR FLOW TO PURGE LEVEL
SET MODE=17 CODE=136 SFE=3,38,77 P=.018 MODE=AIR FLOW TO PURGE LEVEL
SET MODE=18 CODE=1391 SFE=8,38,61 P=.004 MODE=FO FLO LTOFF LVL/LOW STM
SET MODE=19 CODE=1392 SFE=3,33,61 P=.004 MODE=FO FLO LTOFF LVL/NO FLAME
SET MODE=20 CODE=140 SFE=1,31,77 P=.020 MODE=FO RECRC WITH FOTV CLOSED
SET MODE=21 CODE=141 SFE=1,31,77 P=.002 MODE=FO RECRC INHBT SUPPRESSED
SET FUNCTION SWITCHES
PARTS FR=35.4600 QTY=2 RFACTOR=1.10 RF=0.50 SFACTOR=4.60 SF=0.44
SET MODE=1 CODE=1 SFE=1,31,77 P=.185 MODE=LOSS OF PURGE
SET MODE=2 CODE=4 SFE=1,31,77 P=.092 MODE=LOSS OF TRIP
SET MODE=3 CODE=6 SFE=1,31,77 P=.132 MODE=LOSS/INADEQUATE RECRC
SET MODE=4 CODE=131 SFE=10,46,76 P=.671 MODE=LOSS OF BOILER TRIP
SET FUNCTION RELAYS
PARTS FR=1.1523 QTY=2 RFACTOR=1.10 RF=0.50 SFACTOR=4.60 SF=0.30
SET MODE=1 CODE=1 SFE=1,31,77 P=.301 MODE=LOSS OF PURGE
SET MODE=2 CODE=7 SFE=1,31,77 P=.011 MODE=FALSE TRIP
SET MODE=3 CODE=131 SFE=10,46,76 P=.199 MODE=LOSS OF BOILER TRIP
SET MODE=4 CODE=140 SFE=1,31,77 P=.788 MODE=FO RECRC WITH FOTV CLOSED
SET FUNCTION VALVES
PARTS FR=5.5200 QTY=2 RFACTOR=1.00 RF=0.50 SFACTOR=1.60 SF=0.80
SET MODE=1 CODE=6 SFE=1,31,77 P=  .500 MODE=LOSS/INADEQUATE PURGE
SET MODE=2 CODE=127 SFE=4,34,77   .250 MODE=FOTV CLOSES OR CAN'T OPEN
SET MODE=3 CODE=128 SFE=1,31,66 P=.250 MODE=FOTV OPEN OR CAN'T CLOSE
SET GROUP 2 ON
SET BLOCK 2 ON
SET FUNCTION ELECTRONIC/RNR MODULE
PARTS FR=7.6715 QTY=2 RFACTOR=1.10 RF=0.20 SFACTOR=3.25 SF=0.80
```

FIGURE IX-7 (cont)

```
SET MODE=1 CODE=1 SFE=1,31,77 PB,024 MODE=BNR LTOFF LOGIC FAILS
SET MODE=2 CODE=2 SFE=1,31,77 PB,057 MODE=IGNITOR FAILURE
SET MODE=3 CODE=3 SFE=1,31,77 PB,067 MODE=FALSE TRIP
SET MODE=4 CODE=4 SFE=1,31,77 PB,020 MODE=LOSS OF TRIP
SET MODE=5 CODE=5 SFE=1,31,77 PB,008 MODE=FLAME INDICATOR PROBLEM
SET MODE=6 CODE=113 SFE=1,31,66 PB,084 MODE=20 SEC TIMER/TIMES LONG
SET MODE=7 CODE=114 SFE=1,31,66 PB,076 MODE=BNR VLV 5 SEC SHTDN FAIL
SET MODE=8 CODE=115 SFE=1,31,66 PB,051 MODE=BNR VLV 20 SEC SHTDN FAILS
SET MODE=9 CODE=116 SFE=4,34,77 PB,010 MODE=AR CLOSES OR CAN'T OPEN
SET MODE=10 CODE=117 SFE=2,32,66 PB,046 MODE=IGNITOR NOT WITHDRAWN
SET MODE=11 CODE=118 SFE=1,31,77 PB,010 MODE=AR OPENS OR CAN'T CLOSE
SET MODE=12 CODE=119 SFE=3,33,77 PB,010 MODE=BNR VLV CLOSES/CAN'T OPEN
SET MODE=13 CODE=120 SFE=2,32,66 PB,010 MODE=IGNITOR EXTENDED
SET MODE=14 CODE=121 SFE=1,31,77 PB,010 MODE=IGNITOR CAN'T BE EXTENDED
SET MODE=15 CODE=122 SFE=3,33,77 PB,199 MODE=FALSE BURNER TRIP
SET MODE=16 CODE=123 SFE=1,31,66 PB,010 MODE=BNR VLV OPENS/CAN'T CLOSE
SET MODE=17 CODE=124 SFE=4,34,77 PB,018 MODE=BNR FAILS TO TRIP/AR CLOSE
SET MODE=18 CODE=125 SFE=14,46,76 PB,273 MODE=BNR FAILS TO TRP/NO FLAME
SET MODE=19 CODE=126 SFE=16,46,76 PB,017 MODE=BNR FAILS TO TRIP/BNR CLS
SET FUNCTION SWITCHES
PARTS FR=40,6606 QTY=4 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=2 SFE=1,31,77 PB,181 MODE=IGNITOR FAILURE
SET MODE=2 CODE=4 SFE=1,31,77 PB,262 MODE=LOSS OF TRIP
SET MODE=3 CODE=115 SFE=1,31,66 PB,070 MODE=BNR VLV 20 SEC SHTDN FAIL
SET MODE=4 CODE=119 SFE=3,33,77 PB,246 MODE=BNR VLV CLOSES/CAN'T OPEN
SET MODE=5 CODE=122 SFE=3,33,77 PB,141 MODE=FALSE BNR TRIP
SET MODE=6 CODE=124 SFE=4,34,77 PB,070 MODE=BNR FAILS TO TRP/AR CLOSE
SET MODE=7 CODE=126 SFE=16,46,76 PB,070 MODE=BNR FAILS TO TRP/BNR CLS
SET FUNCTION VALVES
PARTS FR=32,7600 QTY=4 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=191 SFE=3,33,77 PB,500 MODE=BNR VLV CLOSES/CAN'T OPEN
SET MODE=2 CODE=231 SFE=1,31,66 PB,500 MODE=BNR VLV OPENS/CAN'T CLOSE
SET FUNCTION RELAYS
PARTS FR=4,3100 QTY=4 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,30
SET MODE=1 CODE=1 SFE=1,31,77 PB,334 MODE=BNR LTOFF LOGIC FAILS
SET MODE=2 CODE=2 SFE=1,31,77 PB,121 MODE=IGNITOR FAILURE
SET MODE=3 CODE=3 SFE=1,31,77 PB,211 MODE=LOSS OF TRIP
SET MODE=4 CODE=121 SFE=1,31,77 PB,334 MODE=IGNITOR CAN'T BE EXTENDED
SET FUNCTION TRANSFORMERS
PARTS FR=0,3400 QTY=4 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=2 SFE=1,31,77 PB=1,000 MODE=IGNITOR FAILURE
SET FUNCTION ACTUATORS
PARTS FR=34,6600 QTY=4 RFACTOR=1,00 RF=0,90 SFACTOR=6,60 SF=0,46
SET MODE=1 CODE=116 SFE=4,34,77 PB,250 MODE=AR CLOSES OR CAN'T OPEN
SET MODE=2 CODE=118 SFE=1,31,77 PB,250 MODE=AR OPENS OR CAN'T CLOSE
SET MODE=3 CODE=120 SFE=2,32,66 PB,250 MODE=IGNITOR EXTENDED
SET MODE=4 CODE=121 SFE=1,31,77 PB,250 MODE=IGNITOR CAN'T BE EXTENDED
SET GROUP 3 ON
SET BLOCK 3 ON
SET FUNCTION ELECTRONIC/COMBUST CNTL BLR PWR LOGIC
PARTS FR=3,6739 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,60
SET MODE=1 CODE=58 SFE=8,38,61 PB,324 MODE=LOW STM PRES
SET MODE=2 CODE=591 SFE=5,35,61 PB,140 MODE=HI STM PRES/STM DUMP ACT
SET MODE=3 CODE=592 SFE=6,34,61 PB,140 MODE=HI STM PRES/RUPTURE TUBE
SET MODE=4 CODE=83 SFE=14,46,76 PB,145 MODE=FALSE ALARM
SET MODE=5 CODE=84 SFE=13,43,72 PB,165 MODE=ALARM FAILS
SET MODE=6 CODE=97 SFE=10,40,61 PB,026 MODE=FALSE TURBINE TRIP
SET FUNCTION TRANSDUCERS
PARTS FR=73,5200 QTY=1 RFACTOR=1,30 RF=0,70 SFACTOR=6,60 SF=0,46
SET MODE=1 CODE=58 SFE=8,38,61 PB,500 MODE=LOW STM PRES
SET MODE=2 CODE=591 SFE=5,35,61 PB,250 MODE=HI STM PRES/STM DUMP ACT
SET MODE=3 CODE=592 SFE=6,34,61 PB,250 MODE=HI STM PRES/RUPTURE TUBE
SET GROUP 4 ON
SET BLOCK 4 ON
SET FUNCTION ELECTRONIC/COMBUST CNTL
PARTS FR=100,6652 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
```

FIGURE IX-7 (cont)

```
SET MODE=1 CODE=421 SFE=3,33,61 PR,040 MODE=LOW FD FLO/LOW STM PRES
SET MODE=2 CODE=422 SFE=4,34,61 PR,040 MODE=LOW FD FLO/FLAME OUT
SET MODE=3 CODE=431 SFE=3,33,61 PR,076 MODE=HI FD FLO/SMOKE
SET MODE=4 CODE=432 SFE=2,32,61 PR,039 MODE=HI FD FLO=/HI STM PRES
SET MODE=5 CODE=433 SFE=6,36,61 PR,016 MODE=HI FD FLO=/EXCSV FD
SET MODE=6 CODE=5A SFE=8,38,61 PR,005 MODE=LOW STM PRES
SET MODE=7 CODE=591 SFE=5,35,61 PR,00A MODE=HI STM PRES/STM DUMP ACT
SET MODE=8 CODE=592 SFE=6,36,61 PR,001 MODE=HI STM PRES/RUPTURE TUBE
SET MODE=9 CODE=A0 SFE=12,42,61 PR,093 MODE=LOSS OF CONTROL/COMR CNTL
SET MODE=10 CODE=A11 SFE=3,33,61 PR,026 MODE=POOR AIR/FD RATIO/SMOKE
SET MODE=11 CODE=812 SFE=6,36,61 PR,02A MODE=POOR AIR/FD /EXCSV FD
SET MODE=12 CODE=R2 SFE=13,43,73 PR,007 MODE=LOSS OF REMOTE MANUAL
SET MODE=13 CODE=1421 SFE=3,33,61 PR,136 MODE=HI COMBUST AIR/SMOKE
SET MODE=14 CODE=1422 SFE=3,33,61 PR,087 MODE=HI COMBUST AIR/FLAME OUT
SET MODE=15 CODE=1423 SFE=3,38,61 PR,082 MODE=HI COMBUST AIR/LOW STEAM
SET MODE=16 CODE=1424 SFE=3,33,61 PR,010 MODE=HI COMBUST AIR/SMOKE
SET MODE=17 CODE=1431 SFE=3,33,61 PR,176 MODE=LOW COMBUST AIR/SMOKE
SET MODE=18 CODE=1432 SFE=6,36,61 PR,057 MODE=LOW COMBUST AIR/EXCSV FD
SET MODE=19 CODE=1433 SFE=8,38,61 PR,021 MODE=LOW COMBUST AIR/LOW STEAM
SET MODE=20 CODE=1434 SFE=4,34,61 PR,031 MODE=LOW COMBUST AIR/BLR TRIP
SET FUNCTION VALVES
PARTS PN=32,7600 QTY=2 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=421 SFE=3,33,61 PR,300 MODE=LOW FD FLO/LOW STM PRES
SET MODE=2 CODE=422 SFE=4,34,61 PR,150 MODE=LOW FD FLO/FLAME OUT
SET MODE= 3 CODE=431 SFE=3,33,61 PR,050 MODE=HI FD FLO/SMOKE
SET MODE=4 CODE=432 SFE=2,32,61 PR,300 MODE=HI FD FLO/HI STM PRES
SET MODE=5 CODE=433 SFE=6,36,61 PR,200 MODE=HI FD FLO/EXCSV FD
SET FUNCTION RELAYS
PARTS PN=0,4359 QTY=2 RFACTOR=1,10 RF=0,50 SFACTOR=6,60 SF=0,30
SET MODE=1 CODE=421 SFE=3,33,61 PR,122 MODE=LOW FD FLO/LOW STM PRES
SET MODE=2 CODE=422 SFE=4,34,61 PR,143 MODE=LOW FD FLO/FLAME OUT
SET MODE=3 CODE=431 SFE=3,33,61 PR,194 MODE=HI FD FLO/SMOKE
SET MODE=4 CODE=432 SFE=2,32,61 PR,092 MODE=HI FD FLO/HI STM PRES
SET MODE=5 CODE=433 SFE=6,36,61 PR,030 MODE=HI FD FLO/EXCSV FD
SET MODE=6 CODE=A0 SFE=12,42,61 PR,204 MODE=LOSS OF CONTROL/COMR CNTL
SET MODE=7 CODE=135 SFE=1,31,66 PR,102 MODE=LOSS OF PURGE/LOW AIR
SET MODE=8 CODE=1421 SFE=3,33,61 PR,041 MODE=HI COMBUST AIR/SMOKE
SET MODE=9 CODE=1422 SFE=3,33,61 PR,031 MODE=HI COMBUST AIR/FLAME OUT
SET MODE=10 CODE=1423 SFE=8,38,61 PR,031 MODE=HI COMBUST AIR/LOW STEAM
SET FUNCTION ACTUATORS
PARTS PN=17,2400 QTY=2 RFACTOR=1,00 RF=0,90 SFACTOR=6,60 SF=0,36
SET MODE=1 CODE=1421 SFE=3,33,61 PR,200 MODE=HI COMBUST AIR/SMOKE
SET MODE=2 CODE=1422 SFE=3,33,61 PR,050 MODE=HI COMBUST AIR/FLAME OUT
SET MODE=3 CODE=1423 SFE=4,38,61 PR,100 MODE=HI COMBUST AIR/LOW STEAM
SET MODE=4 CODE=1424 SFE=3,33,61 PR,150 MODE=HI COMBUST AIR/SMOKE
SET MODE=5 CODE=1431 SFE=3,33,61 PR,050 MODE=LOW COMBUST AIR/EXCSV FD
SET MODE=6 CODE=1432 SFE=6,36,61 PR,050 MODE=LOW COMBUST AIR/EXCSV FD
SET MODE=7 CODE=1433 SFE=8,38,61 PR,100 MODE=LOW COMBUST AIR/LOW STM
SET MODE=8 CODE=1434 SFE=4,34,61 PR,150 MODE=LOW COMBUST AIR/BLR TRIP
SET FUNCTION TRANSDUCERS
PARTS PN=63,8801 QTY=1 RFACTOR=1,30 RF=0,90 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=421 SFE=3,33,61 PR,136 MODE=LOW FD FLO/LOW STM PRES
SET MODE=2 CODE=422 SFE=4,34,61 PR,090 MODE=LOW FD FLOW/FLAME OUT
SET MODE=3 CODE=431 SFE=3,33,61 PR,093 MODE=HI FD FLOW/SMOKE
SET MODE=4 CODE=432 SFE=2,32,61 PR,070 MODE=HI FD FLOW/HI STM PRES
SET MODE=5 CODE=433 SFE=6,36,61 PR,070 MODE=HI FD FLOW/EXCSV FD
SET MODE=6 CODE=142; SFE=3,33,61 PR,167 MODE=HI COMBUST AIR/SMOKE
SET MODE=7 CODE=1422 SFE=3,33,61 PR,080 MODE=HI COMBUST AIR/FLAME OUT
****    ALL TAMPA USERS PLEASE TYPE "INFO TAMPA"    ****
****    ALL USERS DIALING LOCAL STAMFORD NUMBERS    ****
****          PLEASE TYPE "INFO NUMBERS"            ****
MCSI RECON AT 12,31,01 ON  09NOVA2,
SET MODE=8 CODE=1423 SFE=8,38,61 PR,090 MODE=HI COMBUST AIR/LOW STEAM
SET MODE=9 CODE=1431 SFE=3,33,61 PR,219 MODE=LOW COMBUST AIR/SMOKE
SET MODE=10 CODE=1432 SFE=6,36,61 PR,055 MODE=LOW COMBUST AIR/EXCSV FD
SET FUNCTION CONTROLLERS
```

FIGURE IX-7 (cont)

```
PARTS FR=4,9560 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=1421 SFE=3,33,61 PR,149 MODE=HI COMBUST AIR/SMOKE
SET MODE=2 CODE=1422 SFE=3,33,61 PR,371 MODE=HI COMBUST AIR/FLAME OUT
SET MODE=3 CODE=1423 SFE=8,38,61 PR,074 MODE=HI COMBUST AIR/LOW STEAM
SET MODE=4 CODE=1424 SFE=3,33,61 PR,111 MODE=HI COMBUST AIR/SMOKE
SET MODE=5 CODE=1431 SFE=3,33,61 PR,118 MODE=LOW COMBUST AIR/SMOKE
SET MODE=6 CODE=1432 SFE=6,36,61 PR,029 MODE=LOW COMBUST AIR/EXCSV FD
SET MODE=7 CODE=1433 SFE=8,38,61 PR,059 MODE=LOW COMBUST AIR/LOW STM
SET MODE=8 CODE=1434 SFE=4,34,61 PR,089 MODE=LOW COMBUST AIR/BLR TRP
SET GROUP 5 ON
SET BLOCK 5 ON
SET FUNCTION ELECTRONIC/DRUM LVL CNTL
PARTS FR=35,7170 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=341 SFE=3,33,61 PR,395 MODE=HI DRUM LVL
SET MODE=2 CODE=342 SFE=20,50,61 PR,044 MODE=HI DRUM LVL/SPILL TO TURB
SET MODE=3 CODE=351 SFE=4,34,77 PR,244 MODE=LOW DRUM LVL/HLP TRIP
SET MODE=4 CODE=352 SFE=6,36,61 PR,124 MODE=LOW DRUM LVL/HI STM TEMP
SET MODE=5 CODE=353 SFE=6,36,61 PR,042 MODE=LOW DRUM LVL/HI BLR TEMP
SET MODE=6 CODE=A3 SFE=14,14,74 PR,045 MODE=FALSE ALARM
SET MODE=7 CODE=A6 SFE=12,42,72 PR,104 MODE=LOSS OF CONTROL/DRUM LVL
SET FUNCTION TRANSDUCERS
PARTS FR=35,9800 QTY=2 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=341 SFE=3,33,61 PR,115 MODE=HI DRUM LVL
SET MODE=2 CODE=342 SFE=20,50,61 PR,013 MODE=HI DRUM LVL/SPILL TO TURB
SET MODE=3 CODE=351 SFE=4,34 77 PR,035 MODE=LOW DRUM LVL/BLR TRIP
SET MODE=4 CODE=352 SFE=6,36,61 PR,017 MODE=LOW DRUM LV/HI STM TMEP
SET MODE=5 CODE=353 SFE=6,36,61 PR,006 MODE=LOW DRUM LVL/HI BLR TEMP
SET MODE=6 CODE=A6 SFE=12,42,72 PR,518 MODE=LOSS OF CONTROL/DRUM LVL
SET GROUP 6 ON
SET BLOCK 6 ON
SET FUNCTION ELECTRONIC/FW CNTL
PARTS FR=42,7669 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=32 SFE=3,33,77 PR,511 MODE=LOW FD PRES/LOW DRUM
SET MODE=2 CODE=82 SFE=13,43,73 PR,008 MODE=LOSS OF REMOTE MANUAL
SET MODE=3 CODE=A51 SFE=3,33,63 PR,181 MODE=HI FW PRESS/HI DRUM LVL
SET MODE=4 CODE=A52 SFE=7,37,67 PR,181 MODE=HI FW PRESS/HI DRUM LVL
SET MODE=5 CODE=87 SFE=12,42,72 PR,119 MODE=LOSS OF CONTROL/FW PMP
SET FUNCTION TRANSDUCERS
PARTS FR=37,5400 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=32 SFE=3,33,77 PR,327 MODE=LOW FD PRES/LOW DRUM
SET MODE=2 CODE=851 SFE=3,33,63 PR,195 MODE=HI FW PRESS/HI DRUM LVL
SET MODE=3 CODE=A52 SFE=7,37,67 PR,168 MODE=HI FW PRESS/HI DRUM LVL
SET MODE=4 CODE=87 SFE=12,42,72 PR,337 MODE=LOSS OF CONTROL/FW PMP
SET GROUP 7 ON
SET BLOCK 7 ON
SET FUNCTION ELECTRONIC/FW RECRC VLV CNTL
PARTS FR=18,3752 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=27 SFE=4,31,61 PR,155 MODE=FW RECRC VLV OPN/LO DRUM
SET MODE=2 CODE=28 SFE=5,35,61 PR,205 MODE=FW RECRC VLV CLS/PMP FAIL
SET MODE=3 CODE=83 SFE=14,34,74 PR,320 MODE=FALSE ALARM
SET MODE=4 CODE=A4 SFE=13,43,73 PR,320 MODE=ALARM FAILS
SET FUNCTION VALVES
PARTS FR=32,7600 QTY=1 RFACTOR=1,00 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=27 SFE=4,31,61 PR,500 MODE=FW RECRC VLV OPN/LO DRUM
SET MODE=2 CODE=28 SFE=5,35,61 PR,500 MODE=FW RECRC VLV CLS/PMP FAIL
SET FUNCTION TRANSDUCERS
PARTS FR=29,3000 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=27 SFE=4,31,61 PR,671 MODE=FW RECRC VLV OPN/LO DRUM
SET MODE=2 CODE=28 SFE=5,35,61 PR,329 MODE=FW RECRC VLV CLS/PMP FAIL
SET GROUP 8 ON
SET BLOCK 8 ON
SET FUNCTION ELECTRONIC/SHTR STM TEMP CNTL
PARTS FR=64,0354 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,20
SET MODE=1 CODE=60 SFE=11,41,61 PR,363 MODE LOW STM TEMP/AFT STM TRB
SET MODE=2 CODE=61 SFE=3,33,61 PR,227 MODE=HI STM TEMP/RUPTURE TUBE
SET MODE=3 CODE=A2 SFE=13,43,73 PR,201 MODE=LOSS OF REMOT MANUAL
```

FIGURE IX-7 (cont)

```
SET MODE=4 CODE=A3 SFE=14,44,74 P=,080 MODE=FALSE ALARM
SET MODE=5 CODE=A4 SFE=13,43,73 P=,145 MODE=ALARM FAILS
SET MODE=6 CODE=A8 SFE=12,42,72 P=,175 MODE=LOSS OF CONTROL/STM PRES
SET FUNCTION VALVES
PARTS FR=32,7800 QTY=2 RFACTOR=1,00 RF=0,70 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=60 SFE=11,41,61 P=1,000 MODE=LOW STM TEMP/WET STM TRP
SET FUNCTION TRANSDUCERS
PARTS FR=29,3000 QTY=2 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=60 SFE=11,41,61 P=,671 MODE=LOW STM TEMP/WET STM TRP
SET MODE=2 CODE=61 SFE=3,33,61 P=,329 MODE=HI STM TEMP/RUPTURE TUBE
SET FUNCTION SENSORS
PARTS FR=8,8A32 QTY=2 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=60 SFE=11,41,61 P=,250 MODE=LOW STM TEMP/WET STM TRP
SET MODE=2 CODE=61 SFE=3,33,61 P=,620 MODE=HI STM TEMP/RUPTURE TUBE
SET MODE=3 CODE=A8 SFE=12,42,72 P=,130 MODE=LOSS OF CONTROL/STM PRES
SET GROUP 9 ON
SET BLOCK 9 ON
SET FUNCTION ELECTRONIC/STM DUMP CNTL
PARTS FR=13,1357 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=A9 SFE=5,35,61 P=,570 MODE=STEAM DUMP FAILS
SET MODE=2 CODE=901 SFE=8,38,61 P=,091 MODE=STM DUMP VLV PARTLY OPEN
SET MODE=3 CODE=902 SFE=7,37,61 P=,091 MODE=STM DUMP VLV TOTAL OPEN
SET FUNCTION VALVES
PARTS FR=36,0400 QTY=1 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=A9 SFE=5,35,61 P=,506 MODE=STEAM DUMP FAILS
SET MODE=2 CODE=901 SFE=8,38,61 P=,247 MODE=STM DUMP VLV PARTLY OPEN
SET MODE=3 CODE=902 SFE=7,37,61 P=,247 MODE=STM DUMP VLV TOTAL OPEN
SET FUNCTION TRANSDUCERS
PARTS FR=1,0000 QTY=2 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=A9 SFE=5,35,61 P=,500 MODE=STEAM DUMP FAILS
SET MODE=2 CODE=901 SFE=8,38,61 P=,250 MODE=STM DUMP VLV PARTLY OPEN
SET MODE=3 CODE=902 SFE=7,37,61 P=,250 MODE=STM DUMP VLV TOTAL OPEN
SET GROUP 10 ON
SET BLOCK 10 ON
SET FUNCTION ELECTRONIC/FWD FD START/STOP CNTL MODULE
PARTS FR=15,3486 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=33 SFE=2,32,62 P=,260 MODE=STDBY FD STRT/HI FW PRES
SET MODE=2 CODE=94 SFE=5,35,65 P=,331 MODE=FW PMP FAIL DUE TO CNTL
SET MODE=3 CODE=95 SFE=13,43,73 P=,409 MODE=FW PMP AUTO SW FAILURE
SET FUNCTION SWITCHES
PARTS FR=24,5400 QTY=2 RFACTOR=1,10 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=94 SFE=5,35,65 P=,396 MODE=FW PMP FAIL DUE TO CNTL
SET MODE=2 CODE=95 SFE=13,43,73 P=,604 MODE=FW PMP AUTO SW FAILURE
SET GROUP 11 ON
SET BLOCK 11 ON
SET FUNCTION ELECTRONIC/DEAERATOR LVL CNTL
PARTS FR=20,9772 QTY=1 RFACTOR=1,32 RF=0,11 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=24 SFE=2,32,61 P=,472 MODE=HI DEAERATOR/LOW DRUM
SET MODE=2 CODE=25 SFE=3,33,61 P=,469 MODE=LOW DEAERATOR/LOW DRUM
SET MODE=3 CODE=62 SFE=13,43,73 P=,016 MODE=LOSS OF REMOTE MANUAL
SET MODE=4 CODE=92 SFE=12,42,72 P=,043 MODE=LOSS OF CONTROL/DEAERATOR
SET FUNCTION VALVES
PARTS FR=65,5200 QTY=1 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=24 SFE=2,32,61 P=,750 MODE=HI DEAERATOR/LOW DRUM
SET MODE=2 CODE=25 SFE=3,33,61 P=,250 MODE=LOW DEAERATOR/LOW DRUM
SET FUNCTION TRANSDUCERS
PARTS FR=19,1300 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=24 SFE=2,32,61 P=,673 MODE=HI DEAERATOR/LOW DRUM
SET MODE=2 CODE=25 SFE=3,33,61 P=,327 MODE=LOW DEAERATOR/LOW DRUM
SET GROUP 12 ON
SET BLOCK 12 ON
SET FUNCTION ELECTRONIC/FD HEADER TEMP
PARTS FR=20,A022 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=A6 SFE=4,34,77 P=,527 MODE=LO FD TEMP/SMOKE
SET MODE=2 CODE=A6 SFE=3,33,66 P=,377 MODE=HI FD TEMP/POSSL FLASH
SET MODE=3 CODE=62 SFE=13,43,73 P=,096 MODE=LOSS OF REMOTE MANUAL
```

FIGURE IX-7 (cont)

```
SET MODE=4 CODE=93 SFE=12,42,72 P=,043 MODE=LOSS OF CONTROL/FD TEMP
SET FUNCTION VALVES
PARTS FR=36,0500 QTY=1 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=44 SFE=4,34,77 P=,519 MODE=LO FD TEMP/SMOKE
SET MODE=2 CODE=46 SFE=3,33,66 P=,481 MODE=HI FD TEMP/POSBL FLASH
SET FUNCTION TRANSDUCERS
PARTS FR=5,3750 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=44 SFE=4,34,77 P=,372 MODE=LO FD TEMP/SMOKE
SET MODE=2 CODE=46 SFE=3,33,66 P=,413 MODE=HI FD TEMP/POSBL FLASH
SET MODE=3 CODE=93 SFE=12,42,72 P=,215 MODE=LOSS OF CONTROL/FD TEMP
SET GROUP 13 ON
SET BLOCK 13 ON
SET FUNCTION ELECTRONIC/FD RECRC CNTL
PARTS FR=13,0015 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=381 SFE=4,34,77 P=,228 MODE=LOW FD PRES/HLR TRIP
SET MODE=2 CODE=382 SFE=4,34,77 P=,152 MODE=LOW FD PRES/FLAME OUT
SET MODE=3 CODE=39 SFE=11,41,34 P=,620 MODE=HI FD/HI STM PRESSURE
SET FUNCTION VALVES
PARTS FR=33,6600 QTY=1 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,46
SET MODE=1 CODE=381 SFE=4,34,77 P=,297 MODE=LOW FD PRES/HLR TRIP
SET MODE=2 CODE=382 SFE=4,34,77 P=,198 MODE=LOW FD PRES/FLAME OUT
SET MODE=3 CODE=39 SFE=11,41,34 P=,505 MODE=HI FD/HI STM PRESSURE
SET FUNCTION TRANSDUCERS
PARTS FR=0,5000 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=39 SFE=11,41,34 P=1,000 MODE=HI FD/HI STM PRESSURE
SET GROUP 14 ON
SET BLOCK 14 ON
SET FUNCTION ELECTRONIC/LO PUMP CNTLS
PARTS FR=7,1579 QTY=2 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=50 SFE=5,35,61 P=,209 MODE=LO PMP FAIL/LOW LO
SET MODE=2 CODE=96 SFE=13,43,73 P=,791 MODE=LO PMP AUTO SW FAILURE
SET FUNCTION SWITCHES
PARTS FR=20,1300 QTY=2 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=50 SFE=5,35,61 P=,072 MODE=LO PMP FAIL/LOW LO
SET MODE=2 CODE=96 SFE=13,43,73 P=,928 MODE=LO PMP AUTO SW FAILURE
SET FUNCTION RELAYS
PARTS FR=0,5300 QTY=2 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,30
SET MODE=1 CODE=96 SFE=13,43,73 P=1,000 MODE=LO PMP AUTO SW FAILURE
SET GROUP 15 ON
SET BLOCK 15 ON
SET FUNCTION ELECTRONIC/ITC
PARTS FR=136,5641 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=97 SFE=10,40,61 P=,279 MODE=FALSE TURBINE TRIP
SET MODE=2 CODE=98 SFE=10,48,61 P=,098 MODE=AMD/AST VLV SETTING FAILS
SET MODE=3 CODE=99 SFE=19,49,61 P=,108 MODE=LOSS OF CRASH BACK
SET MODE=4 CODE=100 SFE=19,49,61 P=,086 MODE=WRONG AMD/AST VLV OPENED
SET MODE=5 CODE=101 SFE=11,41,61 P=,043 MODE=LOSS OF RATE CHANGE
SET MODE=6 CODE=106 SFE=20,31,61 P=,074 MODE=LOSS OF OVERSPEED TRIP
SET MODE=7 CODE=107 SFE=16,46,61 P=,186 MODE=LOSS OF TURB TRIP
SET MODE=8 CODE=108 SFE=1,50,80 P=,034 MODE=SHAFT STOPPED IN APD
SET MODE=9 CODE=109 SFE=1,50,80 P=,060 MODE=APD IN ONE DIRECTION
SET MODE=10 CODE=110 SFE=20,50,61 P=,172 MODE=LOSS OF MPC
SET FUNCTION SWITCHES
PARTS FR=123,5400 QTY=1 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=103 SFE=13,43,61 P=,028 MODE=LOSS OF TURNING GEAR
SET MODE=2 CODE=107 SFE=16,46,61 P=,628 MODE=LOSS OF TURB TRIP
SET MODE=3 CODE=111 SFE=18,48,61 P=,263 MODE=LOSS OF CONTROL/HYDR FAIL
SET MODE=4 CODE=112 SFE=13,43,61 P=,081 MODE=LOSS OF HANDPUMP
SET FUNCTION VALVES
PARTS FR=129,2400 QTY=1 RFACTOR=1,18 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=97 SFE=10,40,61 P=,124 MODE=FALSE TURBINE TRIP
SET MODE=2 CODE=104 SFE=1,49,61 P=,150 MODE=AST GUARD VLV FAIL CLOSED
SET MODE=3 CODE=105 SFE=1,31,80 P=,255 MODE=DRAIN VLV FAILS CLOSED
SET MODE=4 CODE=111 SFE=18,48,61 P=,409 MODE=LOSS OF CONTROL/HYDR FAILS
SET MODE=5 CODE=112 SFE=13,43,61 P=,062 MODE=LOSS OF HANDPUMP
SET FUNCTION RELAYS
```

FIGURE IX-7 (cont)

```
PARTS FR=25,2500 QTY=1 RFACTOR=1,10 RF=0,50 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=97 SFE=10,40,61 P=,100 MODE=FALSE TURBINE TRIP
SET MODE=2 CODE=94 SFE=19,49,61 P=,024 MODE=LOSS OF CRASH BACK
SET MODE=3 CODE=102 SFE=1,44,61 P=,024 MODE=LOSS OF TRP/ABO RPM +5
SET MODE=4 CODE=103 SFE=13,43,61 P=,012 MODE=LOSS OF TURNING GEAR
SET MODE=5 CODE=107 SFE=16,46,61 P=,840 MODE=LOSS OF TURB TRIP
SET FUNCTION ACTUATORS
PARTS FR=2,3400 QTY=1 RFACTOR=1,00 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=111 SFE=18,48,61 P=1,000 MODE=LOSS OF CONTROL/HYDR FAIL
SET FUNCTION TRANSFORMERS
PARTS FR=20,7000 QTY=1 RFACTOR=1,32 RF=0,22 SFACTOR=3,25 SF=0,80
SET MODE=1 CODE=111 SFE=1A,48,61 P=1,000 MODE=LOSS OF CONROL/HYDR FAIL
SET FUNCTION SENSORS
PARTS FR=263,2000 QTY=1 RFACTOR=1,30 RF=0,80 SFACTOR=6,60 SF=0,44
SET MODE=1 CODE=97 SFE=10,40,61 P=,128 MODE=FALSE TURBINE TRIP
SET MODE=2 CODE=98 SFE=18,48,61 P=,21A MODE=AHD/AST VLV SETTING FAILS
SET MODE=3 CODE=100 SFE=19,49,61 P=,21A MODE=WRONG AHD/AST VLV OPENED
SET MODE=4 CODE=101 SFE=11,41,A1 P=,21A MODE=LOSS OF RATE CHANGE
SET MODE=5 CODE=102 SFE=1,46,61 P=,21A MODE=LOSS OF TRP/ABO RPM +5
SET FUNCTION SOLENOIDS
PARTS FR=25,1700 QTY=1 RFACTOR=1,00 RF=0,90 SFACTOR=11,60 SF=0,86
SET MODE=1 CODE=97 SFE=10,40,61 P=0,526 MODE=FALSE TURBINE TRIP
SET MODE=2 CODE=111 SFE=1A,48,61 P=0,47A MODE=LOSS OF CONTROL/HYDR FAIL
SET FUNCTION PUMPS
PARTS FR=157,6086 QTY=1 RFACTOR=1,60 RF=0,90 SFACTOR=11,60 SF=0,80
SET MODE=1 CODE=111 SFE=1A,48,61 P=1,000 MODE=LOSS OF CONTROL/HYDR FAIL
```

Using these data summaries and the FMEAs, system effects and mission effects can be traced back through the subsystem to the function, and if so desired, to the individual parts. As an example, "Boiler Trip/Correct and Restart Boiler" is the number one contributor to criticality during normal steaming. This accounts for 24.6568 percent of the total criticality. A major contributing subsystem can be determined by observing the percentages in the right-hand column for the same system effect. Examination of the subsystems shows that the burner management master subsystem contributes a total of 5.16 percent of the total and is the highest subsystem. This can be further isolated by examining the functions for the subsystem. For this particular system effect, electronics contribute .024 per cruise and the valves .023. If it is desired to determine which specific electronic circuits are contributing to the system effect, the criticality reference number can be obtained and found in the failure modes summary sheets. The failure modes summary sheets will then reference the individual line items in the FMEA's which contribute to that note number.

Although boiler trip is the most critical during normal steaming, it is not the most frequent system effect. The most frequent system effect is "alarm/activate remote manual" which occurs .4956 times per cruise. Although this system effect occurs on the average once every two cruises, it is ranked fourth as far as criticality because of the minor mission loss probability. Upon examining the system effects for maneuvering, the "alarm/activate remote manual" system effect moves up to first place in criticality with a contribution of 37.9 percent of the total. Because of the comparatively short time span for maneuvering versus normal steaming (20 versus 710 hours), the probability of occurrence decreases significantly. The probability of occurrence drops to .01359 but the mission loss probability increases from .1 for normal steaming to .6 for maneuvering.

Based on the figures in the system effect summary, it could be expected that approximately one time out of 100 while entering or leaving port, the vessel automatic propulsion control would have to be switched to remote manual operation.

Examination of the system data shows that approximately .92 alarms can be expected during normal cruising per month. This is relatively close to what has been reported in the literature search when it is considered this data does not include all of the system alarms. The total system failure rate amounts to approximately 2.6 per month which also compares relatively closely to the 3M data which reported 1.6 per month but did not include valves and actuators.

To summarize the data for Phase I, the top contributor to mission criticality is the possibility of permanent boiler or turbine damage. Other mission effects such as "temporary reduced RPMs" and "small performance degradation" are relatively non-critical during normal steaming and have a relatively small mission loss probability. The possible boiler/turbine damage effect is usually the result of failures which are not properly alarmed. As an example, there is no alarm for low steam temperature, and consequently, wet steam can enter the turbine. During maneuvering, the possibility of boiler/turbine damage drops down to third place with respect to its contribution to criticality. This is because the vessel requires the full maneuvering capability and the two top mission effects, "small performance degradation" and "temporary reduced RPMs", become relatively critical during maneuvering. During phase 3, the light-off phase, a major delay in light-off becomes the top criticality contributor. This would be where manual light-off is required, introducing a good possibility of departure delay. The second ranking contributor to mission criticality is possible boiler damage during this phase. This is mainly because of the potential for explosion during boiler light-offs.

In addition to the analysis of the effects of the three phases, a computer analysis was performed to determine the effects of the adjustment factors. These factors adjust the basic failure rates for temperature, quality, premature failures, and preventative maintenance. The justification for these factors was discussed in Section VI. As previously described, each subsystem is divided into functions for the computer analysis. The functions consist of classes of parts, such as electronic parts, sensors, valves, etc. Each class of parts has a different adjustment factor.

Appendix G contains the input data for the quantitative criticality analysis, and gives the associated factors for each function. Following the input data, the entire computer output for the basic factor analysis is provided. Of the remaining four factor analyses, only the first four subsystems have been included in the appendix. Figures IX-8 through IX-12 are the five systems effect summaries.

The factor analysis was performed for phase one, i.e., the normal cruising phase. In this study, a normal cruising phase of 710 hours, or approximately one month was used. Using a one month period permits a convenient comparison to other literature related to commercial vessels where failures are usually expressed on a per month basis.

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY
18	ERRATIC RPMS/USE HANDPUMP	12	.2475	9.5402
16	LOSS OF TRIP	7	.1897	7.3113
4	BLR TRIP/CORRECT/RESTART BLR	5	.2273	8.7631
11	NO ALARM--ONLY LIGHT/INDICATOR	7	.1747	6.7335
10	FALSE TURB TRP/CORRECT/RESTART	10	.7470E-01	2.8796
3	ALARM/ACTIVATE REMOTE MANUAL	3	.4956	19.1049
6	EXPLOSIVE CONDITION	7	.8323E-01	3.2083
19	ERRATIC DIR CONTROL/USE HDPMP	13	.4640E-01	1.7887
8	MPC REDUCES RPM/CORRECT/RESUME	5	.6228E-01	2.4007
13	LOSS OF BACK-UP OR ALARM	14	.1095	4.2191
20	LOSS OF PROTECTIVE FEATURE	7	.3300E-01	1.2719
7	TURB TRIP--CORRECT/RESTART TURB	10	.1750E-01	0.6745
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.1078	4.1541
14	FALSE ALARM	2	.2956E-01	1.1393
2	NO EFFECT	2	.1147	4.4222
1	NOT APPLICABLE TO THIS PHASE	1	.4948	19.0730
5	AUTO BACK-UP TAKES OVER	2	.8601E-01	3.3153

FIGURE IX-8

System Effects, Basic Failure Rate
and Normal Steaming Phase

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY
16	LOSS OF TRIP	7	.2345	7.4786
4	BLR TRIP/CORRECT/RESTART BLR	5	.2679	8.5449
11	NO ALARM--ONLY LIGHT/INDICATOR	7	.2104	6.7105
10	FALSE TURB TRP/CORRECT/RESTART	10	.9327E-01	2.9748
3	ALARM/ACTIVATE REMOTE MANUAL	3	.6142	19.5911
6	EXPLOSIVE CONDITION	7	.1061	3.3840
19	ERRATIC DIR CONTROL/USE HDPMP	13	.6038E-01	1.9258
8	MPC REDUCES RPM/CORRECT/RESUME	5	.7802E-01	2.4884
13	LOSS OF BACK-UP OR ALARM	14	.1355	4.3224
20	LOSS OF PROTECTIVE FEATURE	7	.4354E-01	1.3888
7	TURB TRIP--CORRECT/RESTART TURB	10	.2098E-01	0.6691
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.1412	4.5028
14	FALSE ALARM	2	.3901E-01	1.2444
1	NOT APPLICABLE TO THIS PHASE	1	.5812	18.5381
18	ERRATIC RPMS/USE HANDPUMP	12	.2783	8.8771
5	AUTO BACK-UP TAKES OVER	2	.1030	3.2855
2	NO EFFECT	2	.1277	4.0735

FIGURE IX-9

System Effects, Temperature Increased to 50° C.
Normal Steaming Phase

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY
11	NO ALARM--ONLY LIGHT/INDICATOR	7	.1201	8.4546
4	BLR TRIP/CORRECT/RESTART BLR	5	.1297	9.1253
16	LOSS OF TRIP	7	.7352E-01	5.1746
10	FALSE TURB TRP/CORRECT/RESTART	10	.4041E-01	2.8444
3	ALARM/ACTIVATE REMOTE MANUAL	3	.2329	16.3918
19	ERRATIC DIR CONTROL/USE HDPMP	13	.3396E-01	2.3900
6	EXPLOSIVE CONDITION	7	.3701E-01	2.6051
8	MPC REDUCES RPM/CORRECT/RESUME	5	.3878E-01	2.7296
13	LOSS OF BACK-UP OR ALARM	14	.4198E-01	2.9543
7	TURB TRIP--CORRECT/RESTART TURB	10	.1095E-01	0.7707
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.5443E-01	3.8310
20	LOSS OF PROTECTIVE FEATURE	7	.7644E-02	0.5380
14	FALSE ALARM	2	.6502E-02	0.4576
5	AUTO BACK-UP TAKES OVER	2	.5207E-01	3.6649
18	ERRATIC RPMS/USE HANDPUMP	12	.1781	12.5343
2	NO EFFECT	2	.8149E-01	5.7351
1	NOT APPLICABLE TO THIS PHASE	1	.2813	19.7987

FIGURE IX-10

System Effects, Quality Increased to Lower Military Grade,
Normal Steaming Phase

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY
11	NO ALARM--ONLY LIGHT/INDICATOR	7	1.299	7.9140
4	BLR TRIP/CORRECT/RESTART BLR	5	1.437	8.7562
16	LOSS OF TRIP	7	.9968	6.0746
10	FALSE TURB TRP/CORRECT/RESTART	10	.4459	2.7170
3	ALARM/ACTIVATE REMOTE MANUAL	3	2.797	17.0455
6	EXPLOSIVE CONDITION	7	.4190	2.5533
19	ERRATIC DIR CONTROL/USE HDPMP	13	.2887	1.7595
8	MPC REDUCES RPM/CORRECT/RESUME	5	.3724	2.2695
13	LOSS OF BACK-UP OR ALARM	14	.5702	3.4744
7	TURB TRIP--CORRECT/RESTART TURB	10	.1258	0.7668
20	LOSS OF PROTECTIVE FEATURE	7	.1095	0.6671
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.5283	3.2195
14	FALSE ALARM	2	.9606E-01	0.5854
5	AUTO BACK-UP TAKES OVER	2	.5493	3.3474
18	ERRATIC RPMS/USE HANDPUMP	12	2.155	13.1343
2	NO EFFECT	2	.9042	5.5099
1	NOT APPLICABLE TO THIS PHASE	1	3.316	20.2056

FIGURE IX-11

System Effects, Premature Failure Rates Used
(First six months of operation)
Normal Steaming Phase

SFE	SYSTEM EFFECT	MFE NO.	SYSTEM EFFECT FAILURE PROBABILITY	PERCENT OF ALL GROUPS FAILURE PROBABILITY
4	RLR TRIP/CURRECT/RESTART BLR	5	.1383	9.1718
16	LOSS OF TRIP	7	.1108	7.3517
11	NO ALARM--ONLY LIGHT/INDICATOR	7	.9385E-01	6.2261
3	ALARM/ACTIVATE REMOTE MANUAL	3	.3175	21.0664
10	FALSE TURB TRP/CORRECT/RESTART	10	.4322E-01	2.8674
6	EXPLOSIVE CONDITION	7	.5583E-01	3.7042
8	MPC REDUCES RPM/CORRECT/RESUME	5	.3517E-01	2.3334
19	ERRATIC DIR CONTROL/USE HDPMP	13	.2230E-01	1.4796
20	LOSS OF PROTECTIVE FEATURE	7	.2616E-01	1.7354
13	LOSS OF BACK-UP OR ALARM	14	.6441E-01	4.2734
7	TURB TRIP--CORRECT/RESTART TURB	10	.1011E-01	0.6707
12	AUTO CONTROL OUTPUT IS ERRATIC	3	.6706E-01	4.4488
5	AUTO BACK-UP TAKES OVER	2	.4703E-01	3.1201
14	FALSE ALARM	2	.2365E-01	1.5687
2	NO EFFECT	2	.6238E-01	4.1387
18	ERRATIC RPMS/USE HANDPUMP	12	.1133	7.5187
1	NOT APPLICABLE TO THIS PHASE	1	.2762	18.3249

FIGURE IX-12

System Effects, Basic Rates Reduced .
As Results of Comprehensive
Preventative Maintenance,
Normal Steaming Phase

The system failure effect summary for the basic failure rates shows "alarm/activate remote manual" to be the highest contributing system effect, accounting for 19.1% of the total. The second ranking system effect is the "not applicable to this phase" and accounts for approximately 19% of the total systems effect. If the "not applicable" is deducted from the total, the "alarm/activate remote manual" accounts for 24% of the total system effect. The expected frequency of "alarm/activate remote manual" for the basic failure rate is .4596 per cruise. When the temperature is changed from 35° C to 50° C, the expected frequency of "alarm/activate remote manual" increases to .6142 per cruise. In order to better depict the effect of the four factors upon the system, Table IX-1 was compiled from the five system printouts. The total expected frequencies, deleting system effects numbers one and two, which are "not applicable" or "no effect", show the total relevant frequencies.

Using the basic failure rates, the expected frequency of relevant problems is approximately two per cruise. Breaking this down to the various system effects, it is apparent that the frequency of occurrence should not be a serious problem during normal cruising. However, when using the premature failure rates, which are approximately six times the basic rates, some of the previously insignificant problems become significant. As an example, system effect number eight, which is "MPC reduces RPM/correct/resume," has an expected frequency, using the basic failure rate of .06 per cruise. Using the premature failure rates increases the frequency to .37, or approximately once in every three cruises. On the other hand, increasing the quality level of the parts from commercial to military grade reduces the expected frequency by approximately 50%. This same reduction also applies to the institution of a comprehensive preventative maintenance program.

The related mission effect for each system effect is given in the column headed "MFE" of the System Effect summary printouts. For system effect number three "alarm/activate remote manual," the associated mission effect is also number three. Figure IX-13 gives the contribution of the mission effects by subsystems. The mission effect for "alarm/activate remote manual" is "small performance degradation." Although this is the number one contributor to the frequency of system effects, it contributes only 8.9% to the total mission criticality. This occurs because this mission effect has a relatively small probability of a total mission loss. The largest contributor to the mission effect "small performance degradation" is the number four subsystem, Combustion Control with 27.8% of the total.

The general conclusions that can be drawn from these statistics are that the relative frequencies of occurrence of system and mission effects for the basic failure rates should

TABLE IX-1

Summary Of How Factors Change The Frequency
Of System Effects - Normal Cruising Phase

Ship B System Effects	System Effect - Frequency Per Cruise (710 Hrs) Basic Rate	Temp 35°C to 50°C	Quality C to M	Premature S to P	Maintenance No to Main
1. Not applicable to this phase	0.4948	0.5812	0.2813	3.3160	0.2762
2. No effect	0.1147	0.1277	0.0815	0.9040	0.0624
3. Alarm/activate Remote Manual	0.4956	0.6142	0.2329	2.7970	0.3175
4. BLR Trip/Correct/Restart BLR	0.2273	0.2679	0.1297	1.4370	0.1383
5. Auto Back-Up Takes Over	0.0860	0.1030	0.0521	0.5493	0.0470
6. Explosive Condition	0.0832	0.1061	0.0370	0.4190	0.0558
7. Turb Trip - Correct/Restart Turb	0.0175	0.0210	0.0110	0.1258	0.0101
8. MPC Reduces RPM/Correct/Resume	0.0623	0.0780	0.0388	0.3724	0.0352
9.	-	-	-	-	-
10. False Turb Trip/Correct/Restart	0.0747	0.0933	0.0404	0.4459	0.0432
11. No Alarm - Only Light/Indicator	0.1747	0.2104	0.1201	1.2990	0.0939
12. Auto Control Output Is Erratic	0.1078	0.1412	0.0544	0.5283	0.0671
13. Loss Of Back-Up Or Alarm	0.1095	0.1355	0.0420	0.5702	0.0644
14. False Alarm	0.0296	0.0390	0.0065	0.0961	0.0237
15.	-	-	-	-	-
16. Loss of Trip	0.1897	0.2345	0.0735	0.9968	0.0111
17.	-	-	-	-	-
18. Erratic RPM's/Use Hand Pump	0.2475	0.2783	0.1781	2.1550	0.1133
19. Erratic DIR Control/Use Hand Pump	0.0464	0.0604	0.0340	0.2887	0.0223
20. Loss of Protective Feature	0.0330	0.0435	0.0076	0.1095	0.0262
TOTAL (excluding 1 and 2)	1.9848	2.4263	1.0581	12.1900	1.0691

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE				
3 SMALL PERFORMANCE DEGRADATION	.6034	23.259	.3951E-01	8.914
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.1764E-02	0.293	0.0002	0.297
-----GROUP -----				
2 BURNER MODULE	.1380	22.866	0.0135	22.767
-----GROUP -----				
4 COMBUSTION CONTROL	.1682	27.869	0.0167	28.081
-----GROUP -----				
5 DRUM LEVEL CONTROL	.1432	23.748	0.0139	23.422
-----GROUP -----				
6 FEEDWATER CONTROL	.4680E-01	7.756	0.0047	7.826
-----GROUP -----				
8 SHTR STM TEMP CNTL	.6084E-01	10.084	0.0060	10.143
-----GROUP -----				
11 DEAERATOR LEVEL CONTROL	.2370E-01	3.927	0.0024	3.965
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.2091E-01	3.466	0.0021	3.499
MFE				
7 POSSIBLE BLR/TURB DAMAGE	.4806	18.525	.2366	35.449
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.3647E-01	7.588	0.0179	7.587
-----GROUP -----				
2 BURNER MODULE	.6501E-01	13.527	0.0318	13.443
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LOC	.1938E-01	4.032	0.0096	4.073
-----GROUP -----				
4 COMBUSTION CONTROL	.3069E-01	6.385	0.0153	6.465
-----GROUP -----				
5 DRUM LEVEL CONTROL	.4231E-01	8.804	0.0210	8.867
-----GROUP -----				
8 SHTR STM TEMP CNTL	.1114	23.228	0.0548	23.102
-----GROUP -----				
13 FD RECRC CONTROL	.1815E-01	3.776	0.0090	3.816
-----GROUP -----				
15 ITC	.1570	32.659	0.0771	32.587

FIGURE IX-13

Contribution of Each Subsystem to Individual Mission Effect
(Using the basic failure ratio and normal steaming phase)

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE				
5 TEMPORARY REDUCED RPMS	.2896	11.164	.1147	17.167
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.4798E-01	16.568	0.0190	16.582
-----GROUP -----				
2 BURNER MODULE	.3918E-01	13.514	0.0155	13.523
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LGC	.4075E-01	14.069	0.0161	14.058
-----GROUP -----				
4 COMBUSTION CONTROL	.3921E-01	13.537	0.0156	13.638
-----GROUP -----				
5 DRUM LEVEL CONTROL	.4998E-01	17.120	0.0198	16.893
-----GROUP -----				
7 FW RECRC VALVE CONTROL	.2761E-01	9.534	0.0110	9.567
-----GROUP -----				
9 STEAM DUMP CONTROL	.7524E-02	2.598	0.0030	2.616
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.2249E-01	7.765	0.0089	7.798
-----GROUP -----				
13 FD RECRC CONTROL	.1534E-01	5.296	0.0061	5.333
MFE				
12 TEMPORARY LOSS OF RPM CONTROL	.2475	9.548	.1437	21.524
-----GROUP -----				
15 TTC	.2475	100.000	0.1437	100.000
MFE				
14 BACK-UP FAILURE	.1095	4.219	.2173E-01	3.254
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LGC	.8364E-02	7.641	0.0017	7.667
-----GROUP -----				
4 COMBUSTION CONTROL	.9967E-03	0.912	0.0002	0.919
-----GROUP -----				
6 FEEDWATER CONTROL	.2429E-03	0.222	0.0000	0.224
-----GROUP -----				
7 FW RECRC VALVE CONTROL	.8175E-02	3.814	0.0008	3.835
-----GROUP -----				
8 SHTR STM TEMP CNTL	.1369E-01	12.508	0.0027	12.518
-----GROUP -----				
10 FWD FP START/STOP CNTL MODULE	.3022E-01	27.609	0.0060	27.575
-----GROUP -----				
11 DEAERATOR LEVEL CONTROL	.2383E-03	0.218	0.0000	0.219
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.7828E-03	0.715	0.0002	0.720
-----GROUP -----				
14 LO PUMP CONTROLS	.3532E-01	32.268	0.0070	32.163
-----GROUP -----				
15 TTC	.1542E-01	14.092	0.0031	14.[illegible]

Figure IX-13

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE*				
10 TEMPORARY DIM	.9220E-01	3.554	.6398E-01	9.584
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LOC	.1175E-02	1.275	0.0000	1.285
-----GROUP -----				
6 FEEDWATER CONTROL	.9974E-02	10.817	0.0070	10.885
-----GROUP -----				
9 STEAM DUMP CONTROL	.7524E-02	8.160	0.0053	8.210
-----GROUP -----				
15 ITC	.7353E-01	79.748	0.0509	79.620
MFE*				
13 TEMP LOSS DIRECTIONAL CONTROL	.4640E-01	1.709	.2735E-01	8.096
-----GROUP -----				
15 ITC	.4640E-01	100.000	0.0273	100.000

Figure IX-13
(Concluded)

not create a great deal of concern. The premature failure rates and the resulting system and mission effects are considerably higher, and should be of concern. However, these rates can be substantially reduced as explained in other sections. If specific system effects and/or mission effects are not considered acceptable, the effect can be traced back through the data and the individual parts or assemblies causing them can be isolated. Once the parts or assemblies contributing to the unacceptable system or mission effect have been isolated, the necessary corrective action can then be taken. Specific techniques for improving reliability have been detailed in Section X. Also, some of the examples of poor reliability practices which have been found through the criticality analysis and other facets of this study are presented in that section.

TABLE IX-1

Summary Of How Factors Change The Frequency
Of System Effects - Normal Cruising Phase

Ship B System Effects	System Effect - Frequency Per Cruise (710 Hrs) Basic Rate	Temp 35°C to 50°C	Quality C to M	Premature S to P	Maintenance No to Main
1. Not applicable to this phase	0.4948	0.5812	0.2813	3.3160	0.2762
2. No effect	0.1147	0.1277	0.0815	0.9040	0.0624
3. Alarm/activate Remote Manual	0.4956	0.6142	0.2329	2.7970	0.3175
4. BLR Trip/Correct/Restart BLR	0.2273	0.2679	0.1297	1.4370	0.1383
5. Auto Back-Up Takes Over	0.0860	0.1030	0.0521	0.5493	0.0470
6. Explosive Condition	0.0832	0.1061	0.0370	0.4190	0.0558
7. Turb Trip - Correct/Restart Turb	0.0175	0.0210	0.0110	0.1258	0.0101
8. MPC Reduces RPM/Correct/Resume	0.0623	0.0780	0.0388	0.3724	0.0352
9.	-	-	-	-	-
10. False Turb Trip/Correct/Restart	0.0747	0.0933	0.0404	0.4459	0.0432
11. No Alarm - Only Light/Indicator	0.1747	0.2104	0.1201	1.2990	0.0939
12. Auto Control Output Is Erratic	0.1078	0.1412	0.0544	0.5283	0.0671
13. Loss Of Back-Up Or Alarm	0.1095	0.1355	0.0420	0.5702	0.0644
14. False Alarm	0.0296	0.0390	0.0065	0.0961	0.0237
15.	-	-	-	-	-
16. Loss of Trip	0.1897	0.2345	0.0735	0.9968	0.0111
17.	-	-	-	-	-
18. Erratic RPM's/Use Hand Pump	0.2475	0.2783	0.1781	2.1550	0.1133
19. Erratic DIR Control/Use Hand Pump	0.0464	0.0604	0.0340	0.2887	0.0223
20. Loss of Protective Feature	0.0330	0.0435	0.0076	0.1095	0.0262
TOTAL (excluding 1 and 2)	1.9848	2.4263	1.0581	12.1900	1.0691

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE				
3 SMALL PERFORMANCE DEGRADATION	.6034	23.259	.5951E-01	8.914
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.1766E-02	0.293	0.0002	0.297
-----GROUP -----				
2 BURNER MODULE	.1380	22.866	0.0135	22.767
-----GROUP -----				
4 COMBUSTION CONTROL	.1682	27.869	0.0167	28.081
-----GROUP -----				
5 DRUM LEVEL CONTROL	.1432	23.740	0.0139	23.422
-----GROUP -----				
6 FEEDWATER CONTROL	.4680E-01	7.756	0.0047	7.826
-----GROUP -----				
8 SHTR STM TEMP CNTL	.6084E-01	10.084	0.0060	10.143
-----GROUP -----				
11 DEAERATOR LEVEL CONTROL	.2370E-01	3.927	0.0024	3.965
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.2091E-01	3.466	0.0021	3.499
MFE				
7 POSSIBLE BLR/TURB DAMAGE	.4806	18.525	.2366	35.440
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.3687E-01	7.588	0.0179	7.567
-----GROUP -----				
2 BURNER MODULE	.6501E-01	13.527	0.0318	13.443
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LGC	.1938E-01	4.032	0.0096	4.073
-----GROUP -----				
4 COMBUSTION CONTROL	.3069E-01	6.385	0.0153	6.465
-----GROUP -----				
5 DRUM LEVEL CONTROL	.4231E-01	8.804	0.0210	8.867
-----GROUP -----				
8 SHTR STM TEMP CNTL	.1114	23.228	0.0548	23.162
-----GROUP -----				
13 FD RECHC CONTROL	.1815E-01	3.776	0.0090	3.816
-----GROUP -----				
15 ITC	.1570	32.659	0.0771	32.567

FIGURE IX-13

Contribution of Each Subsystem to Individual Mission Effect
(Using the basic failure ratio and normal steaming phase)

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE				
5 TEMPORARY REDUCED RPMS	.2896	11.164	.1147	17.187
-----GROUP -----				
1 BURNER MANAGEMENT/MASTER	.4708E-01	16.568	0.0190	16.582
-----GROUP -----				
2 BURNER MODULE	.3914E-01	13.514	0.0155	13.523
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LGC	.4075E-01	14.069	0.0161	14.058
-----GROUP -----				
4 COMBUSTION CONTROL	.3921E-01	13.537	0.0156	13.638
-----GROUP -----				
5 DRUM LEVEL CONTROL	.4958E-01	17.120	0.0196	16.893
-----GROUP -----				
7 FW RECRC VALVE CONTROL	.2761E-01	9.534	0.0110	9.567
-----GROUP -----				
9 STEAM DUMP CONTROL	.7524E-02	2.598	0.0030	2.614
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.2249E-01	7.765	0.0089	7.798
-----GROUP -----				
13 FO RECRC CONTROL	.1534E-01	5.296	0.0061	5.333
MFE				
12 TEMPORARY LOSS OF RPM CONTROL	.2675	9.580	.1037	21.524
-----GROUP -----				
15 TTC	.2675	100.000	0.1037	100.000
MFE				
16 BACK-UP FAILURE	.1095	4.219	.2173E-01	3.254
-----GROUP -----				
3 COMBUST CNTL/BLR DMD LGC	.8364E-02	7.641	0.0017	7.667
-----GROUP -----				
4 COMBUSTION CONTROL	.9987E-03	0.912	0.0002	0.919
-----GROUP -----				
6 FEEDWATER CONTROL	.2429E-03	0.222	0.0000	0.224
-----GROUP -----				
7 FW RECRC VALVE CONTROL	.4175E-02	3.814	0.0008	3.835
-----GROUP -----				
8 SHTR STM TEMP CNTL	.1369E-01	12.508	0.0027	12.518
-----GROUP -----				
10 FWD FP START/STOP CNTL MODULE	.3022E-01	27.609	0.0060	27.575
-----GROUP -----				
11 DEAERATOR LEVEL CONTROL	.2383E-03	0.218	0.0000	0.219
-----GROUP -----				
12 FUEL OIL HEADER TEMP	.7828E-03	0.715	0.0002	0.720
-----GROUP -----				
14 LO PUMP CONTROLS	.3532E-01	32.268	0.0070	32.163
-----GROUP -----				
15 TTC	.1542E-01	14.092	0.0031	14.1[illegible]

Figure IX-13
(Continued)

CONTRIBUTIONS TO MISSION EFFECTS BY: GROUPS

MISSION EFFECT	SYSTEM CRITICALITY PROBABILITY	PCT CONT. TO SYSTEM CRITICALITY	MISSION CRITICALITY	PCT CONT. TO MISSION CRITICALITY
MFE				
10 TEMPORARY DIN	.9220E-01	3.554	.6398E-01	9.580
-----GROUP -----				
5 COMBUST CNTL/BLR DMD LGC	.1175E-02	1.275	0.0000	1.285
-----GROUP -----				
6 FEEDWATER CONTROL	.9974E-02	10.817	0.0070	10.885
-----GROUP -----				
9 STEAM DUMP CONTROL	.7524E-02	8.160	0.0053	8.218
-----GROUP -----				
15 ITC	.7353E-01	79.748	0.0509	79.628
HFE				
13 TEMP LOSS DIRECTIONAL CONTROL	.4440E-01	1.789	.2735E-01	8.936
-----GROUP -----				
15 ITC	.4440E-01	100.000	0.0273	100.000

Figure IX-13
(Concluded)

not create a great deal of concern. The premature failure rates and the resulting system and mission effects are considerably higher, and should be of concern. However, these rates can be substantially reduced as explained in other sections. If specific system effects and/or mission effects are not considered acceptable, the effect can be traced back through the data and the individual parts or assemblies causing them can be isolated. Once the parts or assemblies contributing to the unacceptable system or mission effect have been isolated, the necessary corrective action can then be taken. Specific techniques for improving reliability have been detailed in Section X. Also, some of the examples of poor reliability practices which have been found through the criticality analysis and other facets of this study are presented in that section.

X. RELIABILITY DESIGN AND PERFORMANCE CRITERIA

The reliability design and performance criteria discussed in this section were developed as a subtask of Task III. The overall Task III objective was to translate the results, findings, and observations of Tasks I and II into a baseline of reliability-related information suitable for use by the Coast Guard in its various activities. During this particular subtask of Task III, design and performance aspects were considered from the standpoint of their role in improving reliability and reducing system downtime.

In conducting this subtask, DOVAP evaluated such factors as design practices, operational characteristics, quality provisions, etc., that can impact the reliability of engine room automation systems. A number of candidate areas for improving the probability/effect of engine room automation system failures were identified and categorized. These areas are supported by examples taken from the findings and observations of Tasks I and II, and from information obtained from firms specializing in the repair of engine room automation systems.

A. DESIGN AND PERFORMANCE CRITERIA BASIC OVERALL REQUIREMENT

Among the documents reviewed during the Task I Literature Survey, there is general agreement that, except for Navy applications, reliability factors are seldom considered in any systematic fashion by the U.S. maritime industry*. This was borne out during DOVAP's Task II detailed reliability analyses when a number of questionable reliability features/practices was noted. These ranged from "omissions" (e.g., the lack of any consistent policy for stress de-rating of electronic parts) to the incorporation of hardware configurations that increase the likelihood of serious failure modes (e.g., incorporating redundancy in trip circuitry without regard to the resulting increased potential for "false trips").

Throughout the study, the common denominator of such observations/findings appeared to DOVAP to be a lack of awareness of the causes of unreliability. This is perhaps best illustrated by its obverse. That is, in areas where reliability considerations are generally well-known, few, if any. questionable practices were noted (e.g., "fail safe"--a

*See, for instance, Appendix A Log #116.

well-known concept--appeared to have been implemented with rigorous attention for such off-on devices as relays and solenoid valves).

DOVAP feels strongly, therefore, that the basic underlying requirement for improving the reliability of marine automation systems lies in improving an awareness of the causes of unreliability. Further, this awareness should become second-nature to all involved--designers, inspectors, operators, surveyors, design reviewers, etc.

To assist in improving this awareness, DOVAP has organized the reliability-related design and performance criteria into the specific categories that either cause unreliability or prolong system downtime. Stated another way, these categories provide groupings for approaches to optimize the probability and/or impact of failures.

These categories are defined and described in Section B, THE CAUSES OF UNRELIABILITY, below. The reliability-related design and performance criteria for each category are discussed in Section C.

B. THE CAUSES OF UNRELIABILITY

As can be recalled from the "bathtub" curve (Section II, "Fundamentals of Reliability"), there will be a period of infant mortality, or "burn-in" failures, followed by a steady state period of random failures, followed finally by a period of wearout failures. Improving reliability, or in other words, eliminating the causes of unreliability, involves measures that deal directly with the characteristics of these three periods. These characteristics, together with generalized reliability improvement approaches, are discussed below.

B.(1) Infant Mortality Failures

During the infant mortality period, failures due to design, fabrication, installation, etc., will predominate and gradually taper off as they are weeded-out during "de-bugging" (or, "burn-in"). A prime function of the design review and testing processes is to identify such potential problems and correct them before the equipment is placed in service. If these processes have been thorough, then ideally the check-out period during sea trials would serve to identify problems due to the overall operating environment which could not have been predicted or simulated earlier.

In practice, of course, infant mortality failures are never completely weeded-out by the end of sea trials. Based on a data evaluation in one study (Log #075), infant mortality periods of five months at the ship level were found. For automation

systems, periods of a year, or longer, are not unusual. This implies that failures due to some specific cause can occur months after the ship has gone into service.

A point that DOVAP feels should be emphasized is that systems as complex and complicated as engine room automation systems can never be 100 percent "de-bugged." In complex computer installations, for example, DOVAP is aware of design "bugs" that turned up over two years after installation; such "bugs" usually require some rare, but not abnormal, set of circumstances to trigger them.

Infant mortality, or "de-bugging" failures, can produce potentialy serious effects. Also, since they result from specific causes, they can be expected to recur if the failed item is replaced with an identical spare. Based on such considerations as these, the identification of potential infant mortality failures should receive more attention than is apparently now the case.

As indicated above, a prime function of the design review and testing processes is to identify such potential failures. There are, however, obviously no "cookbook" approaches for achieving this. A useful rule-of-thumb rationale is that a part will fail when its stress exceeds its strength. While this may at first sound simplistic, identifying the stress-strength parameters that can lead to a failure can be difficult, especially in control equipment where "stresses" are often not of the physical-loading type. The stress-strength parameters, for instance, can involve time constants, electrical power or voltage levels, pneumatic pressures, etc. The utility of the stress-strength concept is that it can provide a framework for systematically identifying potentially troublesome areas so that they can be further investigated and corrective actions taken.

Another "aid" for systemetizing the search for potential infant mortality failures involves the use of design review checklists or guidelines.

Whatever means are taken for identifying potential infant mortality failures, experience from similar hardware systems must be drawn from heavily. Also, since most designers "live with" their designs for quite some time, such failures are seldom due to gross errors or mistakes. Identifying them, therefore, requires careful attention to subtleties.

B.(2) Wearout Failures

The far end of the bathtub curve is characterized by an increasing number of failures due to wearout. Theoretically, this implies that all parts of the system will enter the wearout stage at roughly the same time. In practice, system elements with known lifetimes, such as mechanical equipment, will (or

should be) overhauled or replaced before they reach wearout. When not mistreated, electronic parts, on the other hand, tend to exhibit such long lifetimes that it is difficult to determine when they are approaching wearout.

With an adequate overhaul program for such mechanical units as pumps and motors, and with no mistreatment of electronic parts, the prime candidates for wearout failures then, are pneumatic, hydraulic, and electro-mechanical elements (relays, control valves, controllers, switches, sensors, actuators, etc.). The wearout mechanisms involved with such parts include long-term spring constant degradation, contact surface deterioration, aging embrittlement of materials, etc.

While little can be done to preclude eventual wearout, abnormal wearout can be prevented. This can be done during design by identifying and correcting mechanisms that will lead to early wearout (e.g., reducing friction through better means of lubrication, using more durable materials, etc.).

During the operational phase, preventative maintenance programs can prevent or reduce both abnormal and normal wearout failures through refurbishment or replacement. This is discussed in Section XI.

B.(3) Steady State Failures

The center portion of the bathtub curve is characterized by a "steady state" period of random failures. These failures are not due to any known cause (such as design defects, which contribute to infant mortality). During the steady state period, these random failures are as likely to occur during any one incremental "slice" of time as during any other. As time progresses, the probability that a random failure has occurred will increase. In other words, as more "slices" of time accumulate, the likelihood increases that a random failure will have occurred.

An inherent characteristic of this steady state period is that it spans roughly the useful life of the system. This span depends on the system, but periods of ten years are realistic.

The reliability discipline was originally developed in order to improve steady state reliability. In the years since, infant mortality and wearout failures have to some extent come under the purview of reliability on the basis that "a failure is a failure"--whatever its cause. Nevertheless, the theory and practice of reliability are still primarily concerned with the steady state period, and the "tools of the trade" for improving steady state reliability are highly developed.

As can be recalled from Section II (Fundamentals of Reliability), steady state numerical reliability is determined

by the expression:

$$R = e^{-\lambda t}$$ where:

R, the numerical reliability, is the probability that the equipment has NOT failed,

λ is the equipment failure rate (or, the reciprocal of the equipment MTBF) and,

t is the time period of interest in hours.

For complex systems, the system reliability is obtained by properly combining the reliabilities of the individual system elements. Improving reliability, then, involves increasing the probability that the equipment has not failed. This, in turn, involves improving the parameters in the reliability expression. There are five basic approaches for accomplishing this.

1) Reducing the number of parts is the most straightforward approach to improving reliability. Common sense alone indicates that the fewer the parts, the less chance of failure. Expressed in mathematical terms, eliminating parts eliminates their failure rates from the reliability expression.

2) Improving failure rates is another means of improving reliability. This can be accomplished in several ways. For instance, a better grade of parts can be used, or parts can be "de-rated" to reduce operating streses.

3) Since time is a major parameter in the reliability expression, reducing the time factor will improve reliability. In practice, often there is not much that can be done in this area. On occasions, however, it will be found that operating time can be reduced through lowered duty cycles or alternate approaches to operating mode.

4) Reliability can also be improved by reducing the effects of failures. Redundancy is the approach most often utilized for this. If, for instance, one particular "black box" is needed in a system but two are provided, then the system would not fail if one of these "black boxes" failed. Redundancy, however, can introduce adverse effects and should not be used as a cure-all.

5) Finally, reliability can be improved through improved preventative maintenance. This has the effect of improving a part's failure rate either by improving the condition of the part, or by removing and replacing a degraded part before it fails.

B.(4) System Downtime

Regardless of the reliability improvement measures taken, system reliabilities of 100 percent (or, zero-percent chance of system failure) can never be attained in practice. There will always be some probability, even if it is small, that a random failure will occur. For engine room automation systems, it is prudent to minimize the downtime of the controls due to such failures. Again, there are five basic approaches for accomplishing this.

1)Reduce Response Time to a Failure Condition: Restoring the system to normal operation requires first that the personnel responsible for repair must respond to the failure condition. This process is often set in motion by the occurrence of an alarm. This, in turn, requires that adequate alarms be provided to alert personnel to an abnormal condition. Other means of alerting personnel to the existence of an abnormal condition include periodic inspections and review of operating parameters.

2) Improve Hardware Accessibility: It is a well-known concept that the longer it takes to access failed equipment for troubleshooting and repair, the longer the system will be out of service. Nevertheless, areas with some type of restricted accessibility still manage to sneak through the design and layout process.

3) Reduce Troubleshooting Time: In complex systems, troubleshooting time can constitute a large portion of the overall downtime. This can occur even when the technician is intimately familiar with the system, and is provided with the best in the way of documentation and test equipment. Any inadequacy can only lead to longer troubleshooting time.

4) Reduce Repair Time: In general, automation systems are fairly straightforward to repair once troubleshooting has been completed. Significant delays can occur, however, if spares are not readily available.

5) Minimize System Restoration Time: Complex systems in general, and complex automation systems in particular, are seldom restored to service simply upon completion of repairs. Instead, check-out and sometimes recalibration or alignment are required. Depending on the particular system, these can introduce additional delays in restoration time.

C. RELIABILITY DESIGN AND PERFORMANCE CRITERIA

To summarize from the above, reducing the probability of failures and reducing their potential impact requires improved reliability and reduced failure downtime. Five basic approaches are available for accomplishing each of these.

In identifying the reliability-related design and performance criteria, each of these ten basic approaches was utilized as a category for the various criteria recommendations. For each category, applicable "case histories" are first given by case number. A discussion of the category including background, rationale, and recommendations then follows.

C. (1) Reliability Improvement Categories

C. (1)(a) Reduce the Number of Parts:

Case 1; Excessive Interface Parts

On Ship A, an approach that was frequently utilized for signals running from one card to another is depicted in Figure X-1. As can be seen from this figure, the output from card 1 comes from an inverter with an input of resistor R1 and a capacitor to ground. The signal goes to card 2 where its voltage is conditioned by the zener diode and resistor R2 to +6 volts.

Such signal conditioning is often required where the lengths of runs are quite long; for instance, from one rack to another, or even long runs within the same rack. In many cases, however, this arangement was used where card 1 was separated from card 2 by only a matter of a few inches within the same card rack. For such runs, the inverter on card 1 should have sufficient power to drive the signal to card 2 so that the need for the zener and pull-up resistor R2 on card 2 is questionable.

Also, the need for resistor R1 and the capacitor to ground on card 1 between the NOR gate and the inverter is questionable. Such an approach is often used to obtain a time delay, but it was not apparent that a time delay was required in this circuitry.

Most of the failure modes of these parts cause loss of the signal. That is, if R1 or R3 opened, or if the zener or capacitor shorted to ground, the signal would be lost. For the other failure modes of these parts (i.e., if R2, the zener, or the capacitor opened), loss of some filtering or electrostatic discharge protection would occur.

Since this interface arrangement is used for literally hundreds of signals, the three resistors, zener and capacitor must be multiplied by a factor of over 100 to get the total number of parts involved.

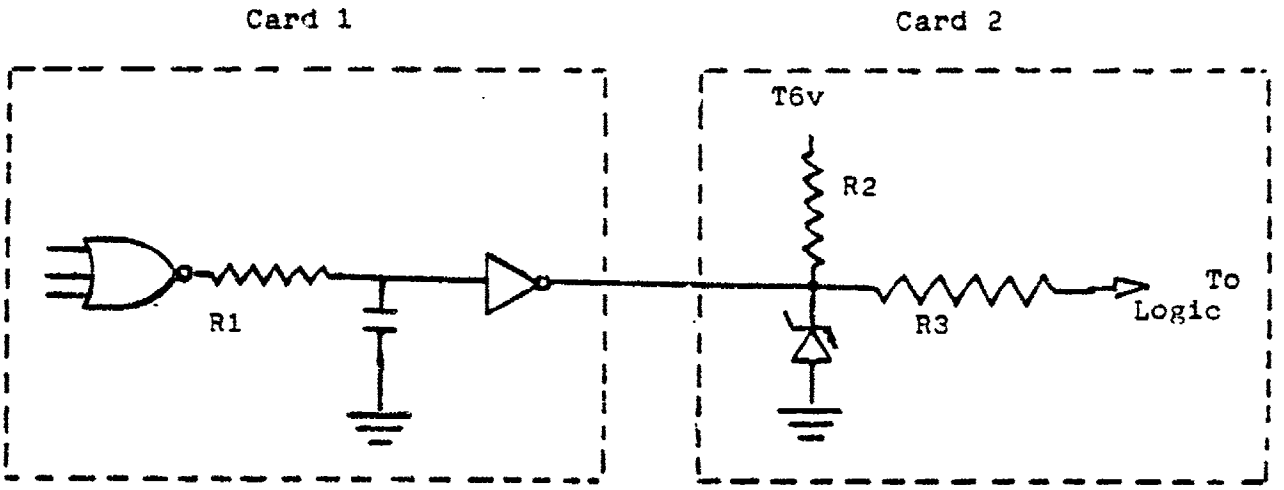


Figure X-1

Excessive Interface Parts

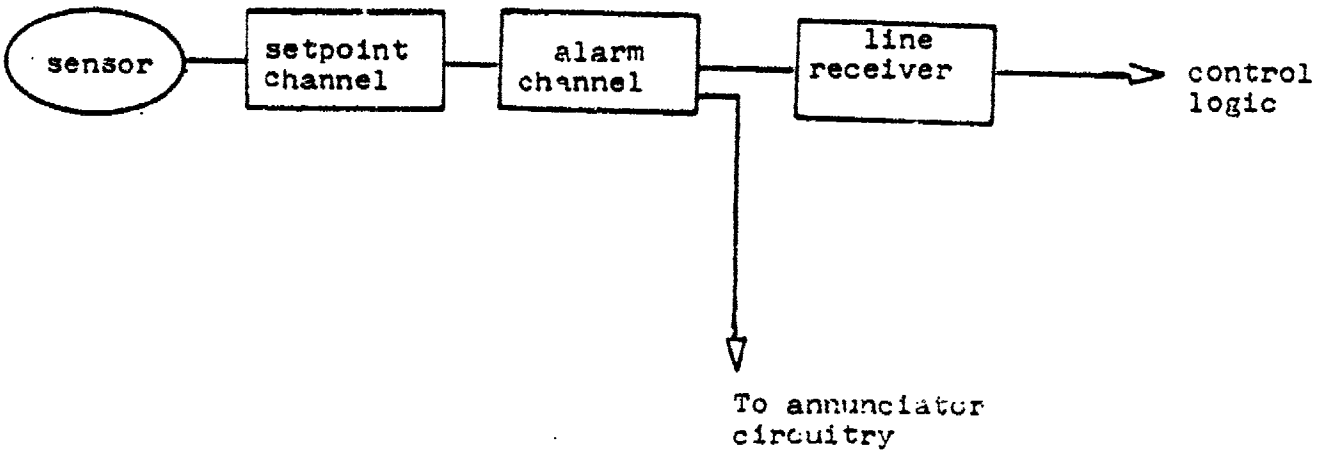


Figure X-2

Excessive Signal Conditioning

Case 2; Excessive Signal Conditioning:

On Ship C, a signal conditioning approach depicted in Figure X-2 was repeatedly utilized. As can be seen from this figure, a signal from a sensor is sent to a setpoint channel on a setpoint printed circuit card. The function of this setpoint channel is to produce an output signal when the signal from the sensor reaches either its high or low limit level. From the setpoint channel, the signal goes to an alarm channel on an alarm card. The purpose of this alarm card is to transmit the alarm signal to the annunciator equipment when the setpoint channel indicates that a signal has reached the alarm level.

From the alarm channel, another signal goes to a line receiver channel on a line receiver card. From the line receiver card, the signal goes to control logic. Examples of such signals would be fuel oil pressure high, lube oil pressure low, etc.

The need for three channels to get from a sensor to an alarm and to the control logic is questionable. The setpoint channel itself puts out a logic level, i.e., the signal goes to a logical 1 condition when the sensor reaches the critical point. When the sensor is not at its critical point, the output of the setpoint channel is a logical 0. Therefore, the logical 1 and 0 conditions needed by the control logic are available at the output of the setpoint channel.

Some portions of the alarm channel are needed to allow the alarm signal to be transmitted to the annunciator circuitry. And again, the logical 1 and 0 conditions needed by the control logic are available at the output of the alarm channel. The line receiver is a further repetition of this, e.g., logic levels are available at its output.

Each one of these "channels" involves a considerable number of parts. Also, this signal conditioning approach is used for many signals. A more reliable approach would be to use the setpoint channel, send the signal from the setpoint channel to the alarm channel only for triggering the alarm annunciator system, and take the logic levels either directly from the setpoint channel or the alarm channel to the control logic. This would eliminate the line receiver channel and possibly part of the alarm channel, with a resulting improvement in reliability. It would also decrease the likelihood of some potentially critical failure effects (e.g., "false" trips) since most failures in any one of these three "channels" would cause the signal level to go to either a logical 0 or a logical 1.

It is possible that some circuit design changes would be required to implement this alternate approach, but the resulting improved reliability would make this effort worthwhile.

Case 3; Inclusion of Unused Parts:

On Ships A, B, and C, cases were noted where "unused" logic circuitry is provided. This was usually to implement some feature not appropriate or necessary for the vessel under consideration. For instance, one case involved gating for status checks of an additional forced draft blower, which was not provided on the vessel. Such provisions allow control system flexibility; i.e., the system does not have to be "tailored" to allow for the specific number of forced draft blowers or whatever. Nevertheless, such logic elements can fail and can have serious failure effects. In the example above, the circuitry had failure modes that indicated that the blower had stopped (even though it was non-existent) which in turn caused the boiler to trip.

Case 4; Excessive Interconnections:

On Ship B, the digital logic is implemented by using printed circuit cards as "building blocks." With this approach, circuit elements on one card must be interconnected with circuit elements on other cards to implement functions and sub-functions. (The alternate approach is to completely implement functions or sub-functions on one card). For the burner master logic, 42 cards were needed to implement the function.

The problem with this approach is the relatively high failure rate associated with printed circuit card interconnects. Failures can occur due to connector contamination, connector contact damage, broken wiring, etc. Such failures can be intermittent and very difficult to troubleshoot. With the use of so many cards, trouble shooting the system can also be difficult. In addition, this approach significantly increases life cycle costs due to the increased number of spares required to maintain the system.

Discussion:

Throughout the analyses of Task II, DOVAP continually noted a lack of awareness of the effects of large numbers of parts. DOVAP therefore feels it should be emphasized that every part has a failure rate and the fewer the parts, the lower the total failure rate.

There are three basic approaches for reducing the number of parts, viz,

a) Alternate design approaches,

b) Elimination of frills,

c) Ascertaining that all parts are really essential.

Cases 1, 2 and 4 above illustrate how the parts count can be reduced through alternate design approaches, i.e., in case 1, interfacing arrangements could be different; in case 2, signal conditioning design could be different. In case 4, logic implementation could be different.

Eliminating frills in order to reduce the parts count is a fruitful area for reliability improvement. Case 3 illustrates one example of this.

Ascertaining that all parts are really essential is illustrated by all four cases discussed above.

Through attention to such aspects as are illustrated in the four cases above, and through an awareness that reliability will be improved through reducing the number of parts, many opportunities for improved reliability will be found.

C.(1)(b) Reduce the Failure Rate

Case 5; Parts Quality Level:

All systems analyzed during Task II utilized an extensive number of commercial grade electronic parts (integrated circuits, resistors, etc.). Many integrated circuits were of the plastic type and were not hermetically sealed, and few were of the quality level where burn-in was performed by the manufacturer. Also, one of the systems utilized pneumatic parts that exhibited few systematic, quality provisions.

Case 6; Electrostatic Discharge (ESD):

There is increasing evidence that many electronic part failures are caused by electrostatic discharge.* A persistent failure problem in Navy equipment, for instance, was found to be due to ESD damage. The causes include discharges occurring when the plastic packaging in which components are shipped is opened; the effects include ESD "punching" through semiconductor junctions. High humidity does not prevent ESD.

*See, for instance, Appendix A Log #034.

Case 7; Part De-Rating:

None of the manufacturers of the engine room automation systems on Ships A, B, and C have guidelines regarding the applied stress on electronic parts, and they do not perform systematic stress analysis. As part of the analysis in Task II, DOVAP did perform such stress analyses for selected electronic parts.

The sample of selected part types represent approximately 20 percent of the card types; however, these are the high usage cards and represent approximately 70 percent of the total parts used in the systems. The circuit analysis performed on these cards determined the power stress ratio, current stress ratio, and junction temperature rise. The results of the circuit analysis, as tabulated below, indicate that the parts on Ship A are more heavily stressed than those on Ship B, and that in neither system are consistent, stress de-rating criteria obvious.

Current and Power Stress Ratios

	Ship A		Ship B	
	Average	High	Average	High
Transistors	.63	.80	.42	.46
Diodes	.08	.16	.05	.10
Capacitors	.32	.69	.11	.20
Resistors	.10	.65	.03	.13

Case 8; Turbine Control Environment:

Although not noted on the systems evaluated during this study, a firm specializing in the repair of marine control systems reports that one of the major problem areas they see involves environmental contamination and heat. They report that turbine controls, in particular, are subjected to oil, water, and soot vapors, and severe swings in temperature.

Case 9; Boiler Front Environment:

The severity of the boiler front environment, with heat, vibration, and contamination being the main culprits, is well known. Nevertheless, marine automation system repair firms report that components not compatible with this environment are not uncommon. Examples include the use of non-high temperature O-rings, the use of metal-to-metal contacts with a propensity for contamination problems, and the use of reed-relays that are prone to "chattering." Also, cases are reported where ventilation is not adequately directed to the boiler front area.

Case 10; Sensor Environment:

A firm specializing in the repair of marine control systems reports that many of the problems it deals with stem from sensor installation. Shock and vibration are significant contributing factors. Electronic sensors, such as process transmitters, are particularly subject to vibration-induced degradation and failure, and should be located in vibration-free areas. Also, sensors on pump discharge lines can experience high shock and vibration levels, and should be mounted on some type of shock absorber.

Case 11; Use of Reed Switches/Relays in Field Environments:

Reed relays and switches, in general, exhibit a high failure rate due to the effects of vibration and should not be used in field applications. An example of the misuse of these devices occurs on Ship B, where they are used on the main and auxiliary condenser for high level indications.

Case 12; Part Types:

On Ship A, the overall approach to the engine room automation system is a hybrid system consisting of digital logic and pneumatic controls. On Ships B and C, the overall approach is a hybrid system consisting of digital logic and analog control loops. In general, for the two steam vessels, where pneumatic control loops are used on Ship A, analog control loops are used on Ship B. This includes feedback loops for steam pressure control, fuel oil flow control, etc.

Discussion:

One of the most fruitful approaches for improving reliability is to improve part failure rates. This can be done in four basic ways:

a) Use higher quality level parts,

b) De-rate parts,

c) Improve the operating environment,

d) Use a different type of part with a better failure rate.

Case 5 above illustrates how failure rates could be improved through use of higher quality level parts. Data from MIL-Handbook 217 indicates that failure rates for commercial parts are 1 to 2 orders of magnitude higher (worse) than those of top level military parts. This occurs because the higher the

quality level of the part, the more effort the manufacturer has put into assuring that defective and potentially defective parts are weeded out before they are delivered. This is primarily accomplished through the use of better materials, more stringent quality control during the manufacture of the part, and through burn-in and testing to screen out infant mortality failures and "weak" parts. Such measures increase the cost of the parts but ensure higher reliability.

In general, for electronic piece parts such as transistors, resistors, and so forth, there are four or five quality levels. The first level is the commerical grade, and these parts utilize inexpensive materials, and are usually sold just as they come off the assembly line. The next quality level involves some part testing and some improvement in the materials and processes used. Subsequent quality levels involve more and more quality assurance provisions by the manufacturer of the part. The highest quality level, i.e., parts with what is called "established reliability," are quite expensive and are warranted only on special military programs for such "one-shot" devices as missile systems. However, the intermediate quality levels are less expensive and produce significant increases in system reliability.

Another quality provision that can increase system reliability involves "weeding out" weak hardware above the piece-part level. Printed circuit cards, for instance, almost always undergo a functional check before they leave the manufacturer. This check is essentially of the "go-no-go" variety, and is generally performed on all cards. In commercial practice, usually only a sampling, if any, cards undergo further burn-in and screening. If ALL cards were subjected to burn-in, those with weaknesses or marginal characteristics exhibited only in circuit operation would be screened out before they had the chance to fail in service.

Another area that comes under the general heading of quality provisions involves protecting electronic piece-parts from electrostatic discharge damage, as indicated in Case 6. The document referenced in Log #034 provides an excellent discussion on the causes, effects, and prevention of ESD. To summarize briefly from that paper, ESD protection involves a two-fold approach that (1) minimizes the use of highly ESD-sensitive devices, and (2) places requirements on the manner in which parts are packaged and handled in order to preclude electrostatic discharge.

As indicated in case 7 above, it was found that little was done in the way of systematically de-rating parts. This de-rating involves parameters unique to each part; for instance, with transistors the major parameter is the power carried by the transistor, and de-rating involves insuring that the part carries only some percentage of the rated value of the parameter. These parameters have been found to be associated with the

failure rate in that the more the appropriate parameter is de-rated, the better the failure rate of the part.

Most formal reliability programs require that electronic parts be de-rated at least 30 percent, and in some cases, over 50 percent is required. While de-rating cannot achieve the dramatic failure rate improvements that can be achieved through the use of better quality parts, it can reduce failure rates by a half or over.

As indicated in case 12 above, systems can be based on various design approaches and hybrid arrangements. In selecting the design approach, reliability can be improved by selecting the type of hybridization that will yield the best failure rates. For instance, failure rates of pneumatic components are quite high and can be over an order of magnitude higher than those for analog circuitry performing the same control function. Similarly, analog circuitry has somewhat higher, i.e., worse, failure rates than those for digital circuitry, but this can be offset by extensive use of digital circuits. That is, if a function can be performed by analog or digital circuitry, the digital circuitry may require many more parts because of the need for extensive gating, flip-flops, etc.

Failure rates can also be improved through improvements in the operating environment. There are some facets of the operating environment that cannot be changed, of course, such as the high humidity levels that shipboard installations will always be subjected to. Some facets of the operating environment are quite amenable to improvement however.

For instance, the effects of shipboard vibration can be reduced by mounting equipment racks on resilient shock/vibration absorbers. The effect of temperature on parts can cause the failure rate to vary by factors of 2 or 3. Therefore, if the operating temperature can be lowered--for instance, through placing the system in an air-conditioned room--failure rates can likewise be improved. The use of fans and heat sinks can also improve the operating temperature of a part.

Where facets of the operating environment cannot be improved, measures can often be taken to improve the hardware's "resistance" to these facets. Such measures would include ensuring the compatibility of mating materials, using high temperature-tolerant components in hot locations, etc. Cases 8 through 11 illustrate situations where component resistance to various environmental facets can be improved.

C.(1)(c) Reduce Operating Time Factors

Discussion:

No cases were found in the analysis where operating time factors could be reduced. However, it can be recalled that reliability is expressed as $R=e^{-\lambda t}$. Therefore, if operating time factors can be reduced, reliability will be increased. This can sometimes by accomplished through lowering the duty cycle. For instance, circuitry that does not have to be on could be switched off, although if this is done, the means of switching should be highly reliable to ensure that the circuitry will indeed switch back on when desired.

Another way of reducing operating time is by alternate approaches to the operating mode. This can sometimes be accomplished during the design stage by considering operating mode possibilities and selecting the one(s) that allow operating time on certain portions of the system to be reduced.

C.(1)(d) Reduce the Effects of Failure

Case 13; Filter Capacitor Failure Modes:

On Ships A, B, and C, each printed circuit card has one or more filter capacitors between each of the card's power inputs and ground. On Ship B, the arrangement is one filter capacitor per power input per card. On Ship A, each power input has from four to eight filter capacitors in parallel (circuit-wise). On Ship C, from five to, in some cases, thirty filter capacitors in parallel are provided.

If any of these capacitors failed open, the card would be more susceptible to EMI from transients on the power line. If any capacitor failed short, however, the power line to ALL cards would be shorted directly to ground. This short would proabably be removed very quickly since the capacitor would, in all likelihood, burn open due to the load it had to carry during this short circuit condition. Nevertheless, the short would keep the power supply shorted to ground long enough to cause trips throughout the system.

From available data on capacitor failure mode ratios, there is a greater likelihood of a capacitor short than a capacitor open. For some electrolytic capacitors, such as those typically used for filtering, the failure mode ratios are about 70 percent for shorts and 30 percent for opens. For a system with 100 printed circuit cards, which is not an especially large system, there would be at least 100 capacitors, implying a non-trivial probability of at least one of them shorting. If, as on Ships A or C, there are five, ten, or more of these capacitors per card, this probability increases dramatically. Over a one-year operating period, computations with the failure rate of these

capacitors indicate over a 50 percent chance of one of them shorting.

These capacitors should be connected in series pairs so that a single capacitor short would not ground the power line. Figure X-3 indicates this arrangement. This "fail safe" approach would require much larger capacitors since series capacitance is an inverse sum, and this could create packaging problems. Nevertheless, the alternative of a high likelihood of a shorted power supply makes the trade-off worthwhile.

Case 14; Fuel/Air Changes on Steam Demand Changes:

On both steam vessels evaluated, the design is such that on an increase in steam demand, the increase in combustion air always leads the increase in fuel oil. Likewise, on a decrease in steam demand, the decrease in fuel oil always leads the decrease in air. This prevents excess fuel oil and the possibility of an explosion. However, certain failure modes were identified where the change in fuel or air would occur in an opposite sequence, thus negating the explosion protection features of the design. Further, no alarms are provided that would alert the crew to this situation if any of these failure modes occurred.

Case 15; Relay Arc Suppression Diodes:

On all three ships, cases were noted where the arc suppression diode across a relay coil consisted of a single diode, as shown in Figure X-4. If this diode shorted, it would short out the relay coil. If the diode opened, arc suppression would be lost but this would not necessarily cause the relay to fail. A more reliable arrangement would be to use two arc suppression diodes in series, as shown in the figure. With this arrangement, if one diode shorted, the relay would still remain operable.

Case 16; Power Supply Redundancy:

Although the systems evaluated during this study had provisions for back-up power, marine automation system repair firms indicate that this is not always the case. The power supplies in question are those that convert ship's power to the specific voltages, usually D.C., required in the control cabinet.

If only one power supply is provided, its failure would cause loss of all automatic control functions. Since control system components will be switching and changing states more frequently during maneuvering, the load on the power supply will be greatest during that operational mode. This implies that a

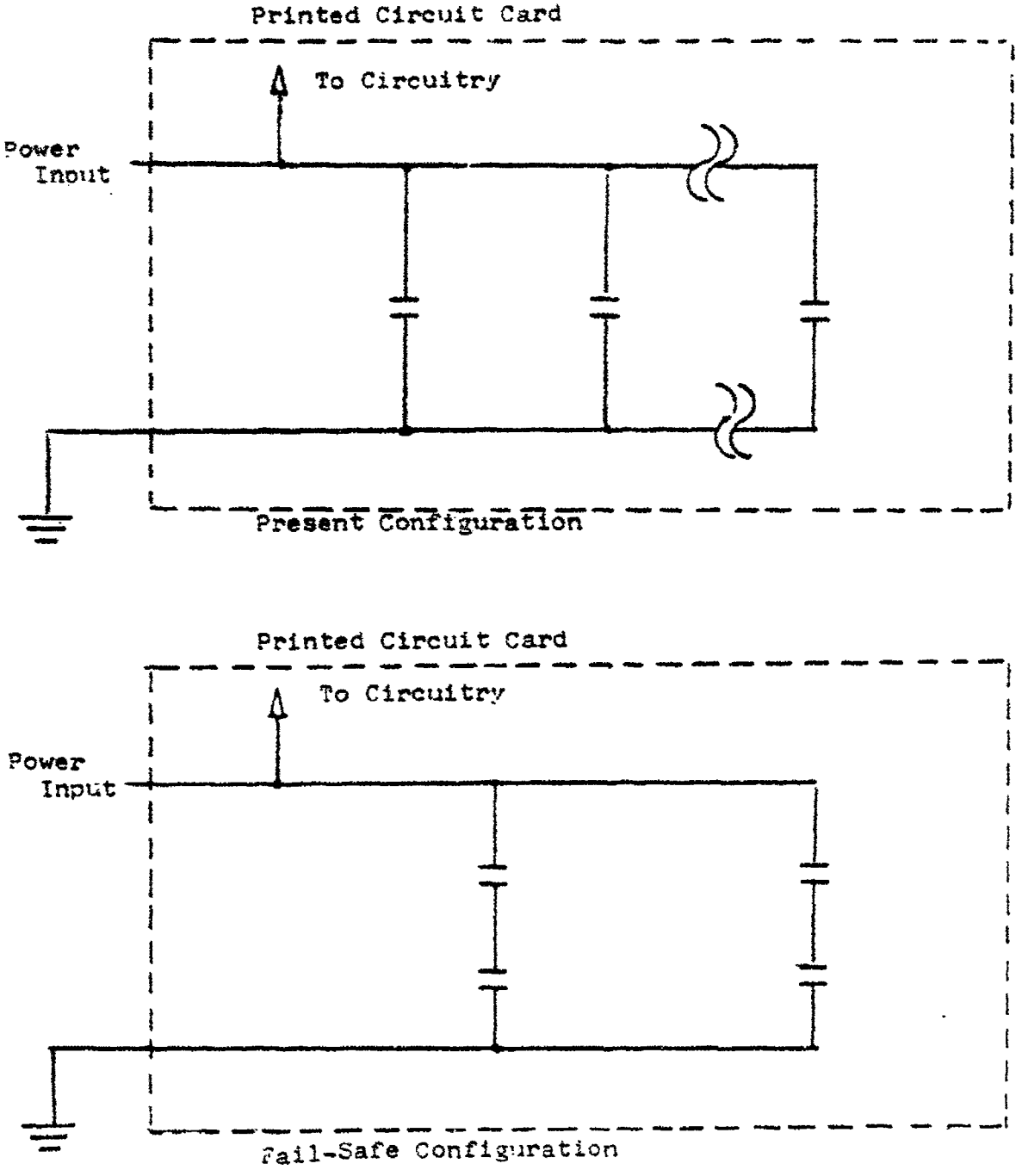
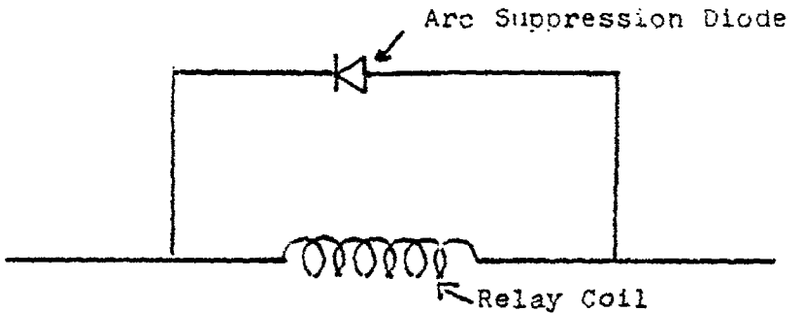
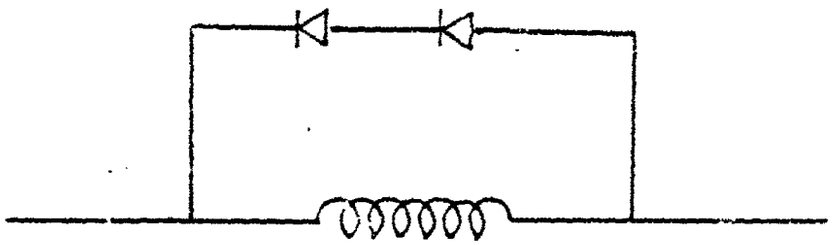


Figure X-3

Printed Circuit Card Filter Capacitors



Present Configuration



Fail Safe Configuration

Figure X-4

Relay Arc Suppression Diodes

power supply would be somewhat more likely to fail during the stresses of the maneuver mode than during other, more benign, modes.

Due to the above risks, redundant power supplies should always be provided and automatic switching from the failed to the back-up unit should be available. Such redundancy is very easy to implement.

Case 17; Common Cause Failures:

The possibility of "common cause" failures did not appear to have been considered in any of the three sytems evaluated. Common cause failures are those where more than one failure mode can be caused by a single failure. An example of a common cause failure would be an integrated circuit composed of several gates, with each gate being used in a different function. If the integrated circuit chip should crack or its power input short, all its gates would fail.

On Ship B, such a common cause failure was found possible. That is, each of three individual circuits on one integrated circuit were used in different functions, viz, ignitor, burner valve, and air register control.

Case 18; Single Point Failures:

The term "single point failure" is reliability jargon for a single failure that causes some catastrophic or highly critical event. In all three systems evaluated, single point failures were identifed. These ranged from single failures that would cause false trips and single failures that would prevent a burner valve from closing in event of a boiler safety trip, to single point failures that would cause an uncommanded vessel speed increase.

Case 19; Sensor Redundancy:

All of the systems evaluated utilized single sensors (i.e., non-redundant). Since the most prevalent sensor failure mode is loss of output, if any of these non-redundant sensors failed, their associated alarm would be lost and any control sequencing circuitry they were used in would malfunction. Protection against such failure consequences could be provided in a straightfoward manner through the use of dual, redundant sensors.

Case 20; Effects of Redundancy:

On all three vessels, the analysis indicated that redundancy was incorporated to ensure that trips occurred when trip conditions existed. The redundancy criteria applied in these cases is to ensure that the crucial event occurs, e.g., that the trip does occur. This is, of course, a valid criteria. On the other hand, such redundancy approximately doubles the number of failure modes that can cause a false event; in this example, a false trip. In other words, each redundant, protective item can generate false protection.

Case 21; Control Failure Due to Problems in External Environment:

The sister ship of Vessel B experienced a total failure of the control system when a water pipe above the control room burst and flooded the controls. During the design and construction of the control room, consideration must be given to the possibility of problems from all external environments, including the possibility of flooding from overhead pipes.

Case 22; Use of a Single Sensor for Multiple Purposes:

On Ship B, there is one steam pressure sensor for each boiler, and the low pressure alarm for each boiler is tied directly to its respective sensor. The outputs from both sensors go to high level select logic, where the higher of the outputs is passed on to all of the following:

a) Steam pressure master control logic
b) Throttle control malfunction proportional control logic
c) Throttle control trip logic
d) Steam dump logic

If one of these sensors failed high, it would cause no alarm because only steam pressure low alarms are provided. Also, the capability would be lost for turbine trip or turbine cutback via the malfunction proportional control for a steam pressure low condition. More significantly, the following chain of events would occur:

a) A high signal would be sent to the steam dump controller, and would activate the steam dump system.

b) A high signal would be sent to the master demand controller, and steam production would be cutback.

c) There would be a sudden decrease in steam with

no turbine cutback from the malfunction proportional control logic and no turbine trip.

d) Eventually, a steam pressure low alarm would occur, but in the interim there would be a tremendous steam inbalance, and a good possibility of loss of other steam dependent systems.

Case 23; Instantaneous Handpump Backup:

A manual handpump is provided as a back-up for the primary throttle controls on both Ships A and B. This handpump should be instantaneously usable because of the possibility of collision if loss of the throttle control occurs. The handpump evaluated in this study, however, requires a minimum of 20 strokes before it can activate the steam valves, and this time could be very critical. An instantaneous back-up should be considered such as an air pump using an accumulator.

Discussion:

In general, there are three ways to reduce the effects of a failure:

a) Redundancy

b) Alternate Design

c) Detect Impending Failures

Cases 13, 15, 16, 19, 22, and 23 above indicate where redundancy could be utilized to reduce the effects of failure. In case 13, the redundancy involves capacitors in series to protect against a shorted capacitor. Likewise, using two diodes across the relay coil in case 15 above involves redundancy protection against a shorted diode. In case 16, power supply redundancy is recommended to prevent loss of control power, and in cases 19 and 22 redundant sensors are advised to preclude loss of the sensor signal. In case 23, an instantaneous back-up to the handpump would be beneficial.

The effects of redundancy, however, can also introduce problems, as indicated in case 20 above. Therefore, in implementing redundancy, trade-offs regarding which failure modes to protect against must be evaluated. In protective circuitry, redundancy approximately doubles the number of failure modes that can cause a "false" protective event. The additional parts in any redundancy approximately doubles the overall failure rate. Also, it is difficult, if not impossible in some cases, to determine when a failure has occurred in a redundant circuit. That is, as long as one redundant counterpart is non-failed, the equipment would perform as required in either a test or actual situation, and it would not be known whether one or both of the

redundant circuits were operable.

Another means of reducing the effects of a failure is to utilize alternate design approaches which eliminate the undesirable failure effect. Case 2 above which discussed alternate approaches to signal conditioning by eliminating the line receivers would involve such approaches. In this case, eliminating the line receiver would also eliminate its failures and therefore, its failure effects. In case 14, an alternate design approach could be derived to eliminate the possibility of fuel oil leading combustion air under certain failure conditions. Likewise, case 21 illustrates how alternate design approaches can preclude problems from external sources.

In cases 17 and 18 above, common cause and single point failures are illustrated. Some, but not all, common cause failures are also single point failures. This occurs because of the multiple failure modes resulting from common cause failures. That is, with multiple failure modes there is increased likelihood that at least one will be critical. Also, there is a good chance that the multiple failure modes will be more critical in combination than any one failure mode would have been singly.

The standard approach to protecting against single point failures usually involves redundancy. Protection against common cause failures is sometimes provided through redundancy and sometimes through alternate design and implementation approaches. In determining which protective approach should be taken for either single point or common cause failures, the trade-offs between redundancy vs. alternate design approaches should be weighed, especially in view of the potential disadvantages cited above for redundancy.

The effects of failure can also be reduced through detecting impending failures. That is, if by some means it is known that a part is going to fail, removing it and replacing it with a good part precludes the possibility that the impending failure would have occurred. This is discussed in the maintenance analysis criteria in Section XI.

C.(1)(e) Provide Improved Preventative Maintenance

Discussion:

Reliability can be improved through preventative maintenance by detecting impending failures, as noted above, and by refurbishing parts to improve their condition. This is discussed in Section XI.

C.(2) Downtime Reduction Categories

C.(2)(a) Reduce Response Time to a Failure Condition

Case 24; Alarm/Indicator Provisions:

In all systems evaluated, considerable attention had been devoted to providing adequate alarms, gauges, and visual indications. Cases were still found, however, where possible abnormal conditions were not "alarmed." On Ship A, for instance, there is a steam temperature high alarm but no steam temperature low alarm. A steam temperature gauge is provided. Neither Ship A nor Ship B has an alarm for high steam pressure. On Ship B, there is no annunciator for ignitor extended.

Case 25; Sensor to Alarm Circuit Path:

On Ship B, most alarm circuits are tied directly to the initiating sensor. Thus, if a failure occurs in circuitry used for a control function, and therefore, not in the "sensor to alarm path," no alarm will occur.

Case 26; Boiler Trip Annunciators:

On Ships A and B, annunciators are provided for boiler trip conditions, and indicate the reason for the trip. The reason indicated, however, does not necessarily include trips caused by the control system. Trips, and their associated alarms occur, for instance, due to low drum level, loss of combustion air, etc. Thus if one of these conditions actually occurs, or appears to have occurred due to a control system failure, the alarm will sound. If the control system fails and causes a trip, but not a trip "covered" by the alarmed trip conditions, no alarm will sound.

Case 27; Position Feedback Sensors:

On all three systems evaluated during this study, and on another system (as reported by a marine control system repair firm), there are cases where a feedback position sensor does not sense the required position directly. That is, rather than sensing the actual position of a valve or actuator, the "element" sensed is a control linkage or servo signal. This would cause no problem as long as no failures occurred. However, if a failure occurred beyond the sensor's "purview," for instance, in the actual actuating device, the control loop would behave as though no failure had occurred, and no annunciator signal would be generated.

Case 28; Critical Alarms Activated by Trip Logic Rather Than the Opening Or Closing of the Valves or Actuators;

On Ship B, the fuel oil trip valve closed alarm is set off by the trip circuitry. However, a substantial amount of circuitry that is not a part of the trip circuitry would close the valve if it failed. Also failure of the valve actuators or the valve itself could cause a valve to close. None of these conditions would alert the crew that the fuel oil trip valve had closed.

Case 29; Inadequate Alarms:

The number and types of alarms were found to vary from ship to ship, however, there generally appears to be inadequate coverage in the following areas:

High Steam Pressure--Although relief valves and the steam dump would prevent a catastrophic problem if high steam pressure developed, it would have been caused by a failure in the steam generation or combustion control system which produces high steam pressure and action should be taken.

Steam Dump--Activation of the steam dump should be alarmed for two reasons, first as redundancy to the high steam pressure alarm. Second, if the steam dump should inadvertently activate, a low steam condition would occur in a relatively short time.

Low Steam Temperature--Low steam temperature could cause turbine damage due to wet steam . This also indicates a failure of the control system for which action should be taken.

Fuel Oil Pressure High-- Fuel oil pressure high could cause excess fuel oil, and corrective action should be taken.

Ignitor Extended--On some systems, there are no lights or alarms to indicate that the ignitor is extended or has not retracted. This could result in significant burner management problems, and should have, as a minimum, an indication light and preferably, an alarm.

Discussion:

It appears to DOVAP that alarm/annunciator provisions are presently based on abnormalities due to factors outside the control system. This is certainly a valid approach, but abnormalities caused by the control system itself should also be covered.

Presently, control system abnormalities are indicated via built-in test circuitry (BIT) on a number of printed circuit cards on all systems evaluated. This BIT usually consists of light-emitting diodes that illuminate when certain control

failures have occurred. However, it seems doubtful that many crew members would be able to, or want to, interpret these BIT indicators. Also, the indications are strictly visual, and are not intended to serve as an alerting-function.

C.(2)(b) Improve Hardware Accessibility

Case 30; Equipment Accessibility:

The portions of control systems that are located within control consoles and racks are almost universally easily accessible. This is not always the case with components remote from the console, such as sensors, actuators, control valves, etc. For instance, on a system not evaluated during this study, the throttle trip valve, which dumps hydraulic pressure in event of a turbine trip, is located inside the turbine front stand. This inaccessibility make maintenance and repair of the valve difficult.

Discussion:

The contribution of ease of accessibility to equipment maintenance is well-known, and most designs attempt to provide adequate working space around equipment. This is not always accomplished, however, as illustrated in Case 30 above. Also, a general area that is often neglected involves the procedures that must be taken to get inside the equipment. For instance, fasteners may be awkward to get to or require special tools.

C.(2)(c) Reduce Troubleshooting Time

Case 31; Loss of Function Due to Failure Outside the Function:

On Ship A, it was found that failures in the purge control circuitry can cause a false boiler shutdown during normal operation (i.e., when no purge is taking place). This occurs because the purge circuitry signals the master fuel oil valve to close during a purge. Therefore, failures in this purge control circuitry can falsely signal the master fuel oil valve to close during normal operation.

Case 32; Documentation Status:

On Ship A, the operator had developed an extensive set of operating manuals. These supplemented the detailed automation system schematics provided by the automation system manufacturer. On Ships B and C, the manufacturers provided extensive operating and schematic documentation. On Ship C, the manufacturer also provided troubleshooting documentation with "quick look" diagrams.

In general, however, none of the documentation appeared suitable for understanding the system without an extensive learning process. Deficiencies noted included; lack of definitions as to the nature of the signals; lack of timing diagrams where timing was an important factor; and lack of adequate signal flow layouts, which made signal tracing difficult.

Case 33; Documentation Not Current:

Because of the large turnover in crew members, maintenance and operational documentation must be current. An example was observed, however, where the manufacturer recommended that the fuel oil pressure alarm sound at 40 psi. It was found during actual operation that the boilers would flame out at 40 psi, so the chief engineer then set the alarm for 45 psi. However, the manual still shows the alarm setting as being 40 psi.

Case 34; Operating Instructions Not Complete:

Any control system limitations should be documented so that crew members are aware of what is normal or abnormal. As an example, when the throttle of Ship B is opened from 40 percent to full ahead, the low steam pressure alarm sounds. The chief engineer reported that this was a normal occurrence but there was no documentation stating that this would occur.

Discussion:

Reducing troubleshooting time implies reducing the time required to locate the failure. This requires a general knowledge of possible failure effects and documentation that enables one to trace the function.

In case 31 above, it could defy reasoning to even consider the possibility that the purge control card had shut the master fuel oil valve. Yet, such obscure types of failures are typical in complex control systems. As discussed in the subsection above, due to the indirect relationship of alarms to the actual failures, the occurrence of an alarm can prove of little use in locating its cause.

As indicated in case 32, troubleshooting diagrams were provided only on Ship C. These utilized a format known as the "quick look." That is, they itemize potential types of failures, such as "Fuel Oil Valve Incorrectly Closes," then list the possible causes for this together with any pertinent troubleshooting instruction. Such troubleshooting aids as this "quick look" documentation would be a valuable asset for every system.

Another area where improved documentation would be of great value involves better definitions for, and identifications of

the logic signals. For instance, on one ship logic signals were referred to by such cryptic abbreviations that it was difficult to tell what these signals were really "doing." A general ground rule for well documented systems is that the signals be identified, their functions listed, and any other pertinent information provided.

Also, with complex digital circuitry as is found in engine room automation systems, logic equations are highly useful both for understanding the system and tracing signals. This is especially the case for NAND-NOR logic that is usually used with integrated circuits since logic relationships are not always clear cut (Figure X-5). Logic equations would indicate the AND-OR relationships required to produce the ultimately desired signal. These logic equations should use well-defined terminology, as just discussed.

Another type of documentation useful for gaining an understanding of a system and for troubleshooting is a programming-type flowchart of the logic flow. In such documentation, the basic requirement is stated in the form of a question in the top-most block, such as "Is purge needed?" The flow chart then proceeds exactly as a computer program flowchart. For example, the block underneath the top-most block would then pose the question, "Has boiler shutdown?"; if yes, then purge would be required, and so forth. This gives a very good indication of the overall logic requirements, and coupled with logic equations, allows the detailed logic to be figured out fairly quickly.

As pointed out in cases 33 and 34, all documentation should, of course, be current and complete.

Reducing troubleshooting time also requires the availability of adequate test equipment and knowledge of how to use it. On the vessels evaluated, it appeared that adequate test equipment had been provided and that at least one crew member on each vessel was knowledgable in its use. However, the literature survey of Task I indicates a general opinion that ships' crews are not trained in the use of test equipment. If troubleshooting consists of removing cards and testing them in a card tester, there is very little that has to be taught in the way of utilizing the equipment. However, if troubleshooting requires the use of more sophisticated test equipment (such as oscilloscopes), more training could certainly be needed.

C.(2)(d) Reduce Repair Time

Case 35; Spare Parts Provisions:

On all three ships evaluated, the automation systems manufacturers originally recommended a complement of spares but indicated that there was little basis for the recommendations.

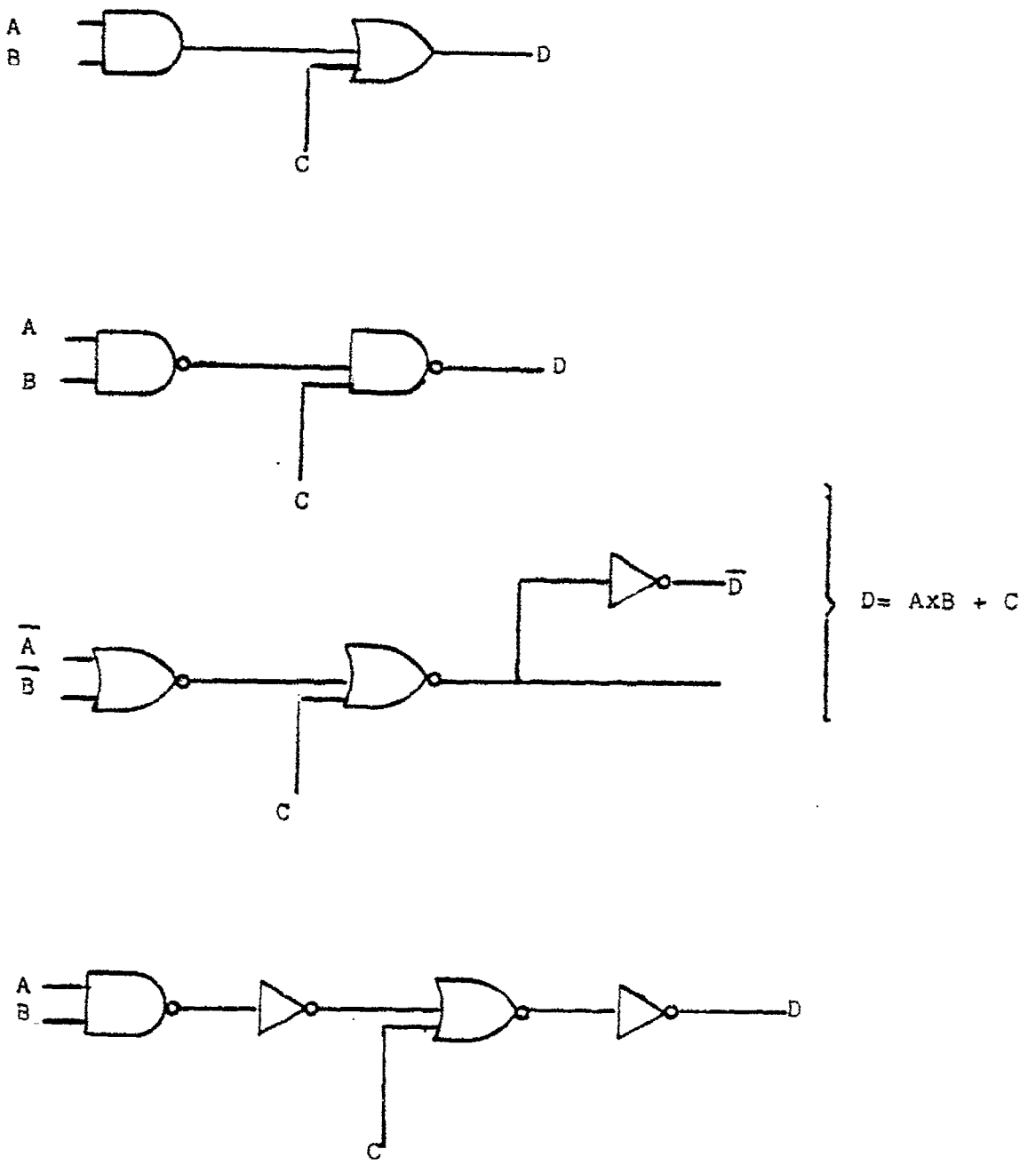


Figure X-5

Alternate Implementations of the Same Logic Functions

On all three vessels the complement of spares was later adjusted to more accurately reflect spare part usage.

Discussion:

Once troubleshooting has identified the cause of the problem, the failed item must then either be replaced or repaired. In either case, spare parts will be required. Therefore, reducing repair time can be accomplished in three ways:

a) Maintaining an adequate supply of spares

b) Ensuring that the spares are readily identifiable and accessible

c) Optimizing the ease of replacement

As a minimum, there should be at least one spare module for each module type. More spares should be available for modules with high failure rates. For determining a "safe" number of spares, a good rule-of-thumb is to compare the module's MTBF with the time required to obtain shoreside replacements. For instance, if it requires two months (about 1,450 hours) to obtain shoreside replacements, and a particular module had an MTBF of about 500 hours, then at least three spares should be available on-board. Ideally, the MTBF used in making this rule-of-thumb comparison should be based on actual, in-service replacement data.

Ensuring that spares are readily identifiable and accessible seems a straightforward, obvious requirement. Optimizing the ease of replacement also seems obvious, and is straightforward where modular approaches, quick disconnects, and the like are possible.

Another requirement, with regard to spares, is that they be operable when called upon for use. This is a self-evident requirement for restoring normal operation following a failure. Also, it is likely that if an engineer had correctly diagnosed a failure, but the spare was inoperable, he would doubt his diagnosis and look elsewhere for the problem.

On Ship A, a system utilized to ensure that spares are operable involves swapping all spares with their operating counterparts at six month intervals. Besides providing assurance that the spare parts are operable, this also keeps them from "lying around gathering dust".

C.(2)(e) Minimize System Restoration Time

Case 36; Electronic Adjustments:

A firm specializing in the repair of marine control systems reports that on a particular turbine control system, a large number of electronic adjustments cause confusion and allow individual interpretation of the set-up of the system. (This system was not one of those evaluated during this study.)

Case 37; Potentiometers:

On Ships A and C, several printed circuit cards have potentiometers which must be set or adjusted to attain proper delay times or voltage functions. The purpose of these potentiometers is to allow a generalized approach to the printed circuit card, i.e., the card can be used on a variety of vessels and the voltage function or time period "trimmed" to suit the particular vessel. Apparently, once these potentiometers are set, they do not need resetting, e.g., the time delay they provide then becomes "set" for the particular vessel.

Discussion:

Minimizing system restoration time implies that once a repair has been effected, the system be put back into service as quickly as possible. This, in turn, implies that the need for calibrations, realignments, checks, etc. be minimized.

As indicated in cases 36 and 37 above, if a card containing a potentiometer or some other type of adjustment was replaced, the replacement card would have to be adjusted. This could take considerable effort of a cut-and-try nature.

There are alternate ways of obtaining time delays and voltage functions that would not require potentiometers or adjustments on the printed circuit cards. If some setting is necessary, it should be provided through some positive means, preferably on a console face (for instance, a knob with a calibrated escutcheon).

XI. MAINTENANCE ANALYSIS

A. BACKGROUND AND HISTORICAL DATA

The effect of maintenance on commercial vessel equipment availability or reliability is difficult to determine from the historical data. During Task I, no documents were found that quantitatively evaluated such effects. The literature did describe preventative maintenance test programs for two ships, the Sugar Islander and the Lash Turkite. The report states that there was a reduction of out-of-service periods and breakdowns, but no quantitative values were given.

One relevant document on this subject is an electrical power industry report entitled, "A Comparative Analysis of PWR Nuclear Plants."* This report evaluates the effects that detailed maintenance plans have on the availability of nuclear reactor plants. The maintenance engineering approach which is described stresses classical reliability and maintainability engineering principles. The paper also points out the necessity of a detailed data base to identify problem areas in which improvements can be made to achieve higher levels of reliability and availability. The conclusion of this paper is that the current availability of Westinghouse domestic plants is approximately 74 percent, and that the target with the detailed maintainability engineering approach is an 8 to 9 percent improvement.

The Navy's approach to maintenance planning and procedures is described in a document entitled "Engineered Marine System Maintenance Extends Life Cycle."** This paper documents the strategy developed by the Navy for insuring the operational readiness of surface combat ships, and discusses the development of engineered maintenance programs for four ship classes. It describes the approach taken to identify and resolve reliability, maintainability, and logistics problems and to define, document, and schedule significant maintenance requirements during the extended operational cycle. A critical part of the engineered maintenance cycle is the documentation of equipment failures that reduce the capability of ship systems.

*1981 Proceedings, Annual Reliability and Maintainability Symposium, S.G. Scaglia, principal engineer, Westinghouse Water Reactor Division, Pittsburgh, PA.

**1982 Proceedings, Annual Reliability and Maintainabililty Symposium, G.A. Lewis, ARINC Research Corporation, Annapolis, Maryland

The results of the Navy's engineering maintenance program are shown in Figures XI-1 and XI-2. Figure XI-1 shows ship availability measured as both a function of total time and maintenance downtime, including scheduled and unscheduled maintenance. This figure includes data on ships participating in the engineered maintenance program as compared to ships that are not. The X axis is time. At the eighth quarter after overhaul, there is a 4.6 percent difference in availability between the ships in the program versus data collected prior to the maintenance engineering program (i.e., on ships not in the program). Figure XI-2 compares the reported problems of ships both before and after participating in the maintenance engineering effort. The plotted lines, which are normalized to the ship's operating time, reflect a 27 percent improvement in the ships that have undergone the engineered maintenance effort.

The Nuclear Plant Reliability Data Report published by the Southwest Research Institute does present quantitative data as to the number of failed parts found during test and maintenance. This was the basis for developing the maintenance reduction factors given in Section VI-B of the report.

As indicated above, there is no quantitative data to show improvements in commercial vessel reliability or availability due to scheduled maintenance. However, there is data from other sources, such as that summarized above, and years of experience in both military and commercial applications that leave little doubt as to the benefits of scheduled maintenance.

B. LOGISTICS SUPPORT ANALYSIS PROGRAM

Logistic support analyses have been required on military programs for many years. The objective of these analyses is to ensure operational readiness, or in other words, an acceptable level of equipment availability. While a military type approach certainly does not seem warranted for commercial vessels, the application of the basic techniques of these support analyses would improve equipment availability. These techniques, and their applicability to commercial vessels, are described below.

a) Maintenance Echelon Analysis: This analysis determines where maintenance is to be performed, i.e., underway, in port, or during lay-up (i.e. "depot").

b) Maintenance Task Analysis: This analysis identifies and defines maintenance task sequences, task times, and task frequencies.

c) Test and Support Equipment Analysis: In this analysis, requirements are identified for on board

FIGURE XI-1

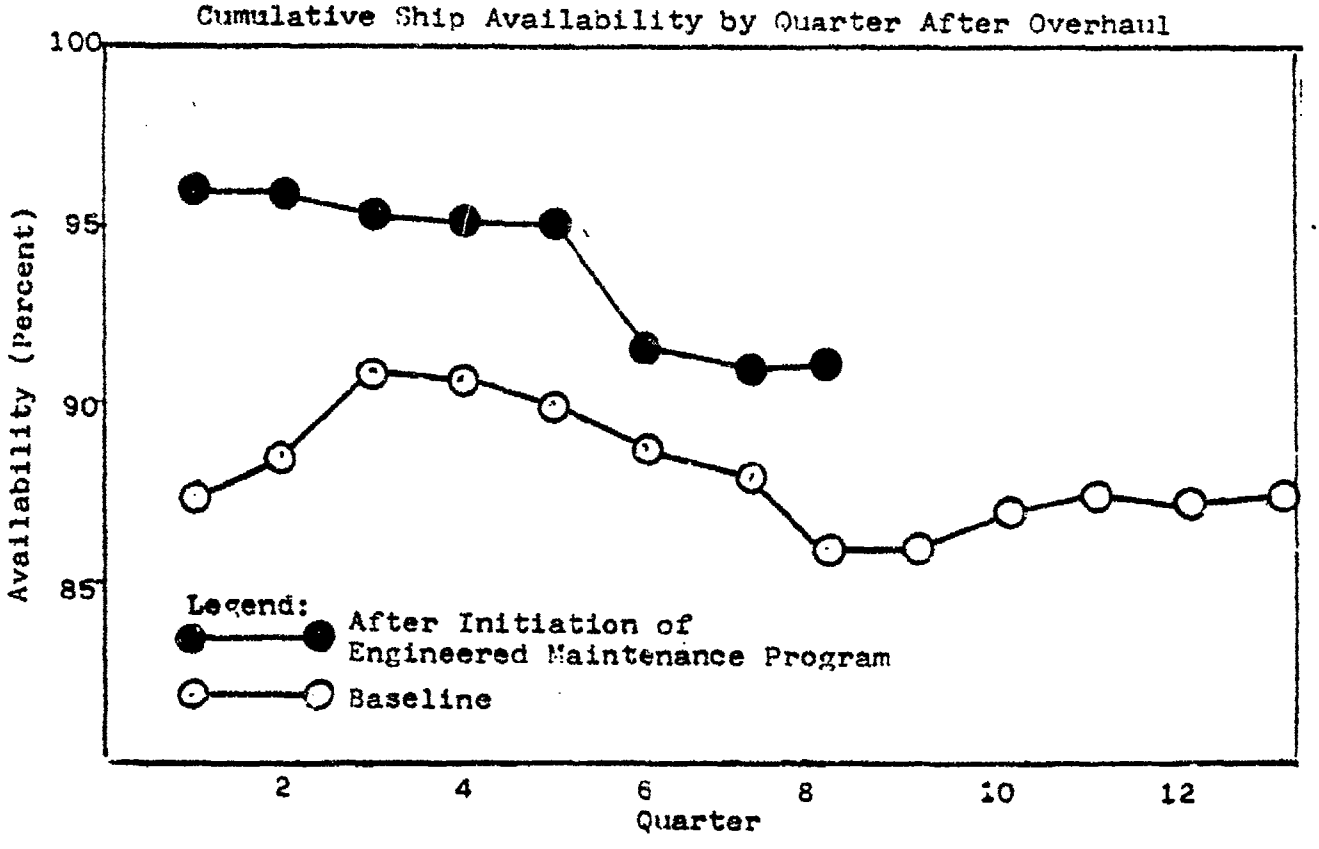
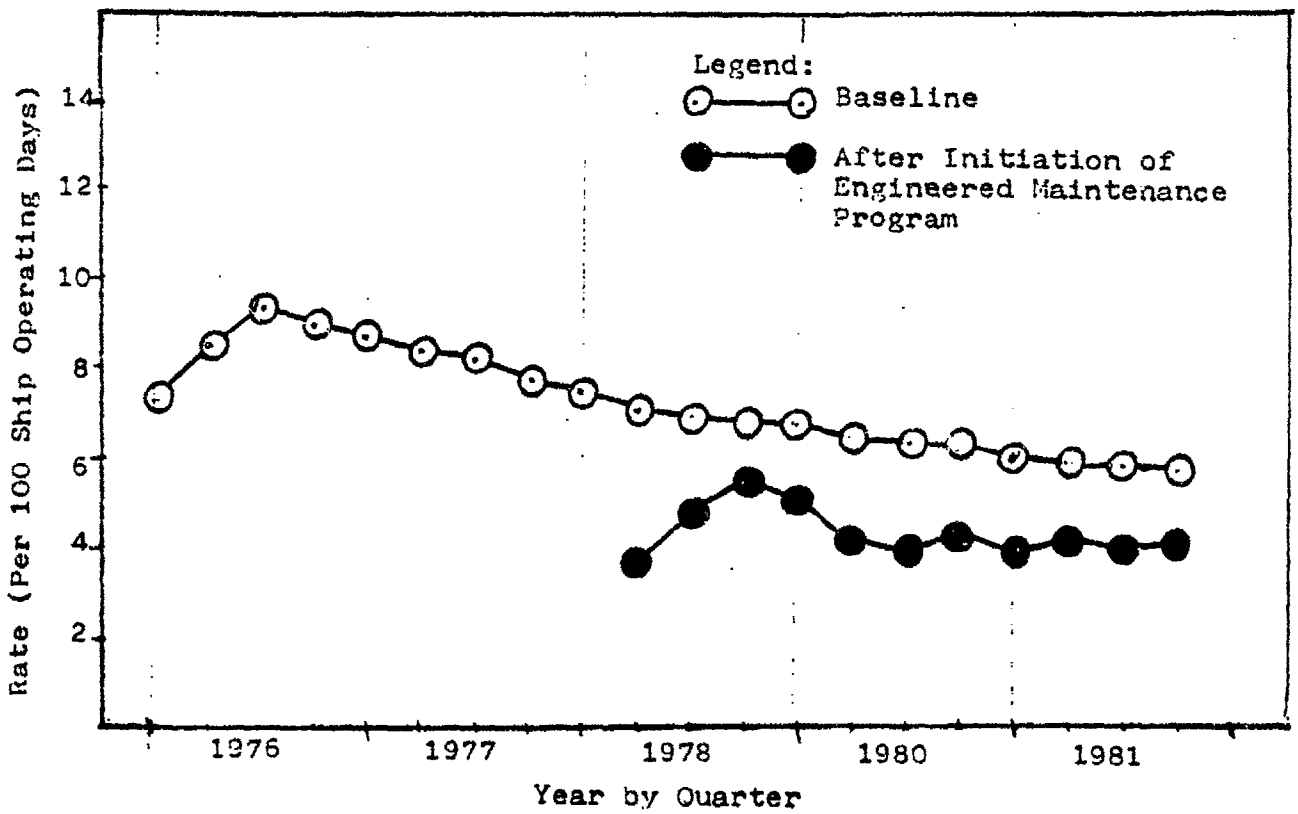

Cumulative Ship Availability by Quarter After Overhaul
100
95
90
85
Availability (Percent)
Legend:
After Initiation of
Engineered Maintenance Program
Baseline
2
4
6
8
10
12
Quarter

FIGURE XI-2

Problem Reporting Frequency



equipment, depot equipment, and back-up equipment such as that which might be provided by technical representatives.

d) Spare and Repair Part Analysis: This analysis determines requirements for on-board spares at the piece part, module, and assembly levels, depot requirements for piece parts, assemblies, etc. pipe line piece part, assembly, etc., requirements, and parts available from supplies and local technical representatives.

e) Personnel and Training Analysis: This analysis evaluates skills and training requirements for on-board crew members, dry dock personnel, and technical representatives.

f) Technical Data Analysis: During this evaluation, the adequacy of manuals, schematics, and catalogs, etc. is assessed.

g) Transportation and Handling Equipment Analysis: This analysis identifies the equipment required to handle large assemblies, and how spares should be packaged so that they will not be degraded due to the effects of the environment and transportation.

h) Facilities Analysis: This effort assesses such factors as the space aboard the vessel, depot facilities, and supplier facilities.

The usual approach when performing a logistics support analysis is first to define the maintenance concept. This concept provides the criteria for subsequent maintenance analyses, and defines overall levels of support, support policies, and desired effectiveness factors, such as availability and reliability. The maintenance concept must consider the total system and the environments in which the system is to operate. All constraints must be defined at this time.

From the maintenance concept, a detailed maintenance plan is then generated. This plan is the working document from which the overall support requirements of the system will be developd. Once the detailed maintenance plan has been developed, logistics support analyses are then performed on individual components and repairable assemblies. A complete logistics analysis is a very exact and time consuming process. Also, a great deal of back-up data is required, such as failure rates, corrective action rates, times to repair, etc.. Nevertheless, certain portions of it could be tailored for use on commercial vessels.

Ideally, each owner/operator would develop an individual maintenance concept and maintenance plan. This plan would be

tailored to the equipment involved and the types of operations being performed. It would define the effectiveness parameters which are critical to operation, and indicate the means to be taken to maximize these parameters. It would then individually evaluate all factors, such as spares, test equipment, crew training, facilities, etc.. A general approach would be to start with system level requirements and apportion them down to subsystems and then to the components and piece parts. The analysis process would then begin in the reverse direction. This would be to evaluate the lowest level of piece parts and generate requirements in the areas of reliability, scheduled maintenance, and non-scheduled maintenance. This would then be repeated for components, subsystems, and then, systems.

C. MAINTENANCE ANALYSIS APPROACH

The maintenance analysis which was performed during this study on the components of automation systems is not a classical analysis as compared to the processes described above.* Because of limitations in the scope of work and the undefined maintenance concept and plans, individual components cannot be evaluated as part of a total integrated program. Frequency and depth of all maintenance actions in many cases are subjected to trade-offs; however, in this study the engine room maintenance cannot be optimized because only a portion of the total engine room equipment was evaluated. Although the automated controls are a very important aspect of the ship's machinery, they require a relatively small portion of the overall vessels' preventative maintenance efforts.

D. PREVENTATIVE MAINTENANCE ANALYSIS

As a subtask of Task III, an analysis was conducted to evaluate preventative maintenance approaches and requirements from the standpoint of their relationship to reliability. This evaluation covered 2 areas. First, the "state-of-the-art" of preventative maintenance practices were surveyed. This focussed on what can, and cannot, be accomplished through preventative maintenance. Second, manufacturers of equipment utilized in the systems covered in this study were contacted to determine their recommended preventative maintenance requirements. Third, preventative maintenance practices and requirements were

*For this study only the preventative maintenance aspects of the total logistic support analysis environment were considered.

analyzed to identify and quantify maintenance-related impacts on part failure rates, This information was then utilized to develop preventative maintenance requirements for both steam and diesel vessels. These 2 areas are discussed in the subsections below.

D.(1) State-Of-The-Art Of Preventative Maintenance

At the present time, control systems can be implemented via 4 basic technological approaches. These are: electronics (either digital or analog), electro-mechanical (relays, solenoid valves, etc.), pneumatics, and hydraulics. Most control systems utilize some combination of these basic approaches. Improvements in the devices within these categories will certainly occur (for instance, microprocessors and very large scale integrated circuits--VLSI--will replace some types of electronic devices currently used). There is no indication, however, that any new type of technological category will be developed in the foreseeable future. Thus, evaluating the state-of-the-art of preventative maintenance practices requires evaluating current practices with each of these approaches.

In the technological category of electronics, preventative maintenance is generally regarded as impossible. That is, there is no way that electronic parts can be refurbished. Also, no systematic, accurate means exist for detecting impending failures in electronic parts, although some electronics technicians maintain that degrading electronic parts are sometimes hotter than normal to the touch.

In the 1950's and early 60's, a preventative maintenance practice commonly used in electronic systems involved marginal power tests. To conduct these tests, the voltage output of the power supply was first increased and then decreased by a slight amount (5% or under). Under each condition, the system was then operated in a functional test mode, with the premise being that "weak" parts would not function properly under marginal power conditions. This approach was abandoned with the advent of integrated circuits.

Today, the accepted approach to "preventative maintenance" of electronic systems is to ascertain that they operate in as benign an environment as possible. To achieve this, adequate cooling through the use of air conditioning, fans, and heat sinks is mandatory. In shock and vibration environments, resilient equipment mounts can be provided for damping. In marine applications, humidity control can sometimes be used to decrease the severity of the environment.

In non-electronic equipment, lifetimes can be predicted with a reasonable degree of certainty. This allows the equipment to be retired or overhauled before wear-out. Electronic parts, on the other hand, exhibit such long lifetimes that it is

difficult to determine when they are approaching wear-out. The communication system on one U.S. spacecraft, for instance, is still performing properly 15 years after launch.

Electrolytic capacitors are probably an exception to this long lifetime trend. A firm specializing in the repair of marine automation systems reports that it frequently encounters "worn-out" electrolytic capacitors. To avoid in-service problems, this firm replaces all control system electrolytic capacitors while the ship is in lay-up.

The one other exception known to DOVAP is connectors. These are prone to such damage as bent contacts from mating-de-mating, or to increased contact resistance due to dirt or corrosion. These items, too, should be inspected during lay-up and cleaned or replaced as necessary.

In the electro-mechanical technological category, preventative maintenance is possible but is all too often neglected. Items in this category include relays, contactors, console switches, limit switches, many types of actuators and sensors, solenoid-actuated valves, etc.. In many cases, manufacturers of such devices recommend specific maintenance actions.

Devices in this category share 2 major characteristics: they usually utilize contacts, and most handle currents in the ampere (as opposed to milli-amp) range. This implies that the contacts and the wiring, wiring terminals, and junction points should be kept in good working order.

Except for devices in sealed containers, contacts should be inspected on the order of every 2 months. More frequent inspection is warranted if the devices are in an oily or dirty environment. Contacts should be cleaned, and checked to determine that they open/close properly. Contacts switching large loads or any inductive load can be subjected to arcing and subsequent pitting and welding, and the entire device should be replaced if this is noted. If the contact device is in a sealed container that is difficult to open, and if the seal is intact, it is probably better left alone.

Wiring and wiring points should be inspected for signs of wear, accumulations of dirt, oil, or corrosion, and indications of potential opens/shorts. Insulation should also be checked for signs of deterioration. Such inspections should be conducted annually for devices in benign environments. Inspection frequencies should be on the order of every 2 months if the device is subject to heat, vibration, or contamination.

Other candidate electro-mechanical areas for routine inspections are actuating mechanisms, which often involve some form of spring tension. Actuating mechanisms should be checked for signs of over-travel, under-travel, and general "looseness". All electromechanical devices should be checked to determine

that they are securely mounted.

Finally, since electro-mechanical devices are subject to wear-out, they should be replaced before they reach end-of-life. The replacement interval can be determined from manufacturer's information, if available, or from experience.

The pneumatic technological category is another area where preventative maintenance is possible. The foremost requirement in this area is maintaining a clean, dry air supply. This, in turn, requires regular attention to filters and dryers.

Many pneumatic devices will have some type of gasket, O-ring or seal that requires periodic replacement. Manufacturers usually provide replacement recommendations for such items.

Many pneumatic devices will also have some type of bellows or diaphragm that can be subject to degradation. By observing operation for signs of "sloppiness" or "sluggishness", this can sometimes be detected without tearing the device down.

Visual inspections of pneumatic devices can sometimes reveal potential failures. For instance, if the body of the device shows signs of corrosion, there may also be internal corrosion that could cause problems. Impending defects in pneumatic tubing are sometimes indicated by stress cracks, and can be detected visually.

All pneumatic connections should be checked for tightness at least twice a year. If the device is in a high vibration area, checks should be made more frequently.

Many pneumatic devices, especially if they are at all complicated, will have a set of very specific manufacturer's maintenance recommendations. These should, of course, be followed.

Pneumatic devices are also subject to wear-out, and should be replaced at the proper time.

Maintenance requirements and practices in the hydraulic technological category are generally similar to those for pneumatics.

The oil should be kept clean, which implies attention to filters. Gaskets, O-rings, seals, etc., should be periodically replaced. Devices should be visually inspected, and hydraulic lines should be kept tight. Manufacturer's recommendations should be followed, and devices should be replaced before they approach wear-out. The hydraulic oil supply should obviously be kept at the proper level.

An area unique to hydraulics concerns its power capability. That is, it is usually used for manipulating large mechanisms or

large loads. In addition, in applications such as turbine steam valve control and CPP control, the "manipulations" must be within tolerances. During layup, all hydraulic elements subject to wear should be inspected, and replaced or repaired if they are out-of-tolerance.

D.(2) Steam Control System Preventative Maintenance

To identify control system preventative maintenance requirements, DOVAP evaluated part classes and part types as separate entities to define the best maintenance approach for the individual part classes and types. Recommendations were developed with respect to maintenance that should be performed on propulsion system controls, parts, and assemblies. However, these recommendations should be modified and/or adjusted from the standpoint of integrating the piece parts recommendations into the total ship machinery maintenance plan.

The maintenance of individual parts is broken down into inspection, test, and preventative maintenance. These are defined as follows:

(a) Inspection: This involves scheduled visual inspection of the hardware and includes inspection for leaks, cracks, corrosion, etc. Many failure modes are visually detectable long before the part degrades to the point of functional failure.

(b) Test: This could be the test of an entire subsystem or of individual components. Where possible, alarms and safety systems should be checked by creating a true abnormal situation. For example, boiler level alarms should be checked by a real increase or decrease of the drum level until the boiler shuts down. This demonstrates that the complete chain of the safety circuit is operable. When testing the alarms, all of the components in some alarm circuits cannot be tested (for example, the main turbine overspeed trip or actual rotor displacement).

(c) Preventative Maintenance: This could be the scheduled replacement of seals, filters, etc., the cleaning of pneumatic parts, or the removal of corrosion from contacts.

The preventative maintenance functions listed below are the general actions which should be taken for each class of parts used in automated propulsion control systems. Specific recom-

mendations provided by the suppliers or the system manufacturer should be followed.

D.(2)(a) Actuators, Pneumatic:

a) Drain traps, every watch.

b) Inspect every 2 months.
Inspect air supply, clean, dry, no contamination.
Inspect filters for dirt, contamination.

c) Test yearly.
Stroke actuator with test input.

D.(2)(b) Alarms:

a) Periodic testing every 2 to 6 months depending upon criticality.

b) When feasible the entire alarm circuit should be tested including the sensor. This should be done either by clearing the system through the alarm trip points or by isolating the sensors and simulating the sensor stimulus.

c) When only testing alarm circuits, input signals should be simulated or tested for opens from the field.

D.(2)(c) Connectors:

a) Inspect every 6 months.
Inspect for corrosion, contamination, bent pins, moisture, loose connections, frayed cable.

b) Preventative maintenance as required. Remove corrosion, contamination, etc.

D.(2)(d) Horns:

a) Test daily.
Test operation by simulating alarm condition.

D.(2)(e) Ignitor:

a) Inspect weekly.
Check carbon rod and pad for contamination and corrosion.

D.(2)(f) Pneumatic Control Devices:

a)
1) Low Select
2) High Select
3) I/P Convertor
4) Controller
5) Square Root Extractor

b) Test yearly.
Check operation with test signals and gauges.

c) Maintenance;
Replace diaphrams as required, maximum time between replacement, 5 years.

d) Overhaul as required.
Shipyard overhaul items.

D.(2)(g) Pneumatic Differential Pressure Transmitter:

a) Test yearly.
Check calibration with test pressure and guage. Monitor remote indicator to ensure same indication as local gauge.

b) Maintenance monthly.
Flush sensing lines to remove contamination.

c) Overhaul as required.
A shipyard overhaul item.

D.(2)(h) Pneumatic Filters:

a) Inspect monthly.
Check for contamination, moisture, replace as needed.

D.(2)(i) Pneumatic Pressure Regulator:

a) Inspect water trap for dry air daily.

b) Test every six months.
Output pressure for proper setting.

c) Preventative Maintenance.
Replace diaphram as needed or maximum of 5 years.

D.(2)(j) Printed Circuit Board Assemblies:

a) Inspect every six months;
Connectors for corrosion, contamination, or wear.

b) Test yearly.
Test spares using card tester.

D.(2)(k) Power Supplies:

a) Inspect every 3 months.
Inspect for signs of over temperature.
Inspect for moisture.
Inspect for contamination.

b) Test and tune yearly.
Test voltages at prescribed test points.

c) Tune system .

D.(2)(l) Pumps:

a) Inspect every 6 months.
Inspect for corrosion, leaks, signs of heat damage, switches for contamination and wear.

b) Test monthly
Test automatic back up switching.
Switch to back up in order to have equal operating time on each pump.

c) Test every six months.
Pressure switches.

d) Overhaul as required

D.(2)(m) Switch, Level:

a) Inspect every 6 months.
Loose connections, frayed wiring.

b) Test yearly.
System check for proper level activation.

c) Preventative Maintenance, every 6 months.
Clean/replace electrodes if needed.

D.(2)(n) Relay:

a) Inspect 6 months to a year (critical relays every 6 months).
Contacts for arcing, contamination.

b) Preventative Maintenance.
Clean contacts or replace relays as required.

D.(2)(o) Switches, Limit:

a) Inspect monthly.
Check connections, check actuating device for wear, corrosion, and contamination.

b) Test every 6 months.

D.(2)(p) Switch, Pressure:

a) Inspect every 6 months.
Open cover, check diaphram for leaks, moisture.

b) Test yearly.
Test with system pressure or test pressure kit.

D.(2)(q) Tranducers, Resistance Temperature Device:

a) Inspect every 6 months.
Open connection box, check for contamination, corrosion, heat deterioration of cable, loose connections, frayed wires.

b) Test yearly.
Disconnect wire at console. Measure resistance against specification. Check for grounds. Check for high resistance junction. Zero and span signal condition circuit.

D.(2)(r) Transmitters:
1) Flow
2) Level
3) Pressure

a) Inspect every 6 months.
Open cover and inspect for signs of damage, water, corrosion, connections loose, wiring frayed.

b) Test yearly.

Zero and span with pressure kit and guages.
(Pressure transmitter).

D.(2)(s) Valves, Hydraulic
Throttle Control:

a) Inspect every 2 months.

b) Test monthly.
Check during throttle tests for leakage or sticking.

c) Overhaul.
Pressure test for leaks during shipyard overhaul.

D.(2)(t) Valves, Pneumatic Control:

a) Inspect every 2 months.
Inspect shaft for binding.
Inspect body for cracks, leaks, corrosion, etc.

b) Test yearly.
System test. Observe for flow when valve closed or break up stream and introduce pressure.
Check for leaks downstream.

c) Preventative maintenance.
Disassemble and inspect; replace worn parts.
Adjust packing nut.
Lubricate per manufacturer's recommendations.
Corrosion - prevention as required.

d) Overhaul.
Stroke valve during shipyard overhaul.
Rework or replace seat if required.
Replace packing if required.
Replace other worn parts.

D.(3) Diesel Control System Preventative Maintenance

On the diesel vessel evaluated during this study, the following items were identified as candidates for preventative maintenance:

a) throttle levers

b) solenoid valves

c) pneumatic air supply

d) relays

e) switches

f) tachometer generator

g) sensors

Most of the control system is electronic, and therefore not amenable to preventative maintenance. The above items form a very small portion of the system in terms of numbers of parts, but they have potentially critical failure modes.

The rationale for the preventative mainenance actions identified for the above items is discussed in general terms in section D(1) above (for instance the need for inspecting contacts). Other specific information not discussed above is provided below for each of the items.

D(3)(a) Throttle Levers:

These are actually large potentiometers with limit switches at their extreme positions. There are throttle levers or potentiometers for bridge control, engine room control, cruise mode trim, and split mode operation. One of these will be continuously energized for operation when the vessel is underway.

Maintenance Items:

a) Inspect limit switches to the extent possible.

b) Inspect wiring.

c) Inspect potentiometers for signs of wear to the extent possible.

D.(3)(b) Solenoid Valves:

a) Inspect wiring.

b) Inspect pneumatic connections.

c) Visually inspect valves for signs of degradation.

d) Perform periodic functional check to determine that valve operates properly (Some of these valves, such as the engine start or stop solenoid valves, will go for periods of days or weeks without being activated during normal operation)

D.(3)(c) Pneumatic Air Supply:

a) Maintain clean, dry air supply.

D.(3)(d) Relays:

a) Inspect contacts where possible.

b) Inspect wiring.

c) Perform periodic functional checks of relay boards to determine that all relays energize/de-energize properly (many of the relays on the relay boards will go for long periods without being used during normal operation).

D.(3)(e) Switches:

a) Inspect contacts where possible

b) Inspect wiring.

c) Perform periodic functional checks of seldom used switches.

D.(3)(f) Tachometer Generator:

a) Inspect wiring.

b) Inspect for signs of wear to the extent possible.

c) Inspect contacts to the extent possible.

d) Lubricate per manufacturer's recommendations.

e) Periodically verify correct calibration.

D.(3)(g) Sensors:

a) Inspect contacts to the extent possible.

b) Inspect wiring.

c) Periodically verify correct calibration.

d) Check mounting.

e) Inspect for signs of wear.

f) Perform periodic functional checks of seldom activated sensors.

XII. MISCELLANEOUS STUDY OBSERVATIONS

During the course of the study, several observations were made that were either of a general nature or not specifically applicable to any single study task. These observations concern the following topics:

a) Environmental Consistency

b) Atomizing Steam Source

c) Technology Approach

d) Operational Aspects

e) Fault Trees vs. FMEA's

f) Wiring

Each of these are discussed below.

A. ENVIRONMENTAL CONSISTENCY

In discussions throughout this report, the effect of the operating environment on reliability and failure rates has been indicated. In conducting the various analyses of the study, DOVAP noted however that environmental requirements were often inconsistent. For instance, the vibration limits called out by ABS for automation systems differ from those called out by IEEE. Temperature limits were also noted as being inconsistent. For instance, on Ship A, the documentation for the various printed circuit cards calls out different temperature extremes for different cards; e.g., one card is reported to be rated for operation at 60° C., another at 30° C., and other cards at temperatures somewhere in between.

These temperature limits should certainly be consistent but more important they should reflect the actual temperature conditions the equipment will be operating under. Assuming that the engine control room is air conditioned (which it should be), an ambient temperature of roughly 25° C. would be expected. Temperature rises of 10° C. are common within equipment consoles. Thus, a temperature limit of at least 35° C. would be realistic, and another 5° to 10° would be desirable for a safety margin.

B. ATOMIZING STEAM SOURCE

On ships A and B, the atomizing steam supply is taken from the de-superheated steam header. This is apparently the case on many steam vessels. No problems were reported due to this on the vessels evaluated, but problems due to wet atomizing steam on another vessel have occurred. Taking the atomizing steam supply off the superheated steam header would permit better control and preclude problems with wet steam.

C. TECHNOLOGY APPROACH

It seems reasonably certain that in the foreseeable future, engine room automation systems will never consist of a "pure" technological approach (for instance, "pure digital, "pure" pneumatic, etc.). Instead, the systems are more likely to consist of hybrid approaches involving some combination of digital/analog, digital/pneumatic, etc. For instance, the automation system on Ship A is primarily digital/pneumatic; Ship B is digital/analog with some pneumatics; Ship C relies heavily on analog control loops with some digital circuitry. Hydraulics will also continue to be used in control systems, especially in areas requiring large mechanical driving forces, such as control of the steam valves in the throttle system. In the paragraphs that follow, some of the overall reliability/failure characteristics of these possible control approaches are discussed.

A major, overall reliability characteristic of any hybrid system involves potential problems at the interfaces between the differing technological approaches. For instance, it is well known that the interface between electronic control circuitry and either pneumatic or hydraulic actuators, valves, etc., can produce many problems. This was borne out in Task I in that such problems were often recorded in the literature. Also, it has been DOVAP's experience on other projects that interface compatibility requirements are often difficult to define precisely. Oversights are common, and there is often inadequate communications between the various disciplines involved. All in all, this is a major area that should be stressed during design review activities.

Since digital integrated circuits are readily available and relatively inexpensive, it seems likely that most control systems will utilize them to the extent possible. The major characteristics that impact the reliability of digital controls can be summarized as follows:

a) Since digital devices are binary, i.e., off/on, failures tend to cause them to "crash," so that there is little margin for graceful degradation. That is, failures tend to cause the signal to go to a "true" or "false" logic level which, in turn, causes the remainder of the processing to either

stop or go into some abnormal state. If the failed signal is infrequently used in the control process, it may not immediately cause this type of effect. Sooner or later, however, when the signal is needed in the process, such effects can be expected.

b) Digital integrated circuits involve almost exclusively NAND/NOR logic. Instead of AND/OR logic where the inputs are combined directly to obtain the desired signals, NAND/NOR logic inverts to produce a "not AND" or "not OR" signal. This means that either NAND or NOR gates can be used to obtain either AND or OR functions, depending on the logic levels of the input signals. (See Figure X-5 in the documentation discussion.) This can complicate the understanding of digital control systems because it can be difficult to see the exact relation that the designer has implemented. To determine the exact function that is being implemented, the logic levels of the signals at the input must be examined, then the subsequent cascaded gates considered (for instance, whether a NAND is feeding a NOR or whatever). The impact of this on troubleshooting is discussed in Section X. Lack of understanding of the system can also hinder design review activities.

c) There is little room for human error in a digital control system. Since it is analogous to a computer that has been programmed, if any human error or abnormal condition causes a signal to erroneously go to some particular state, the control system will do what it is "programmed" to do when this signal state occurs.

Despite these potentially serious failure effect characteristics in digital circuitry, digital integrated circuits have among the lowest failure rates of any type of hardware. One integrated circuit chip, for instance, typically has a failure rate roughly equivalent to one transistor, but recall that the integrated circuit replaces several transistors in the circuit design.

Analog circuitry has somewhat higher failure rates than digital circuitry. Mechanical-type hardware, on the other hand, has significantly higher failure rates than either type of electronic approach. Pneumatic devices, for instance, have failure rates an order of magnitude or more higher than electronic parts.

D. OPERATIONAL ASPECTS

a) On Ship A, it was noted that purge is not possible from the boiler local panel. When the boiler is being lit from the local panel, an additional engineer is required at the engine room console to initiate the purge, and communciations as to the status of the purge are required between the engineers. This seems an unsafe approach. It should be possible to purge from the local panel if the boiler is being lit from the local panel. DOVAP realizes that this could be difficult to implement but the safety trade-offs would indicate that it is warranted.

b) On all the systems evaluated, some indications are provided on the bridge in the form of visual or audible alarms to indicate that certain critical failures have occurred. While these indications do alert the bridge to such critical failures as turbine trip, there are no provisions to alert the bridge to near or potentially critical conditions, (such as the loss of one boiler). It seems that the bridge should be informed that the engine room is not capable of operating at full capacity. Or, in other words, the bridge should automatically be alerted that it could not call on the engine room for the full range of non-failed system capabilities.

c) The systems evaluated during this study had adequate boiler front indicators for visually monitoring air, fuel, and water. This is apparently not always the case. A firm specializing in marine automation system repair recommends that the necessary gages, sight glasses and periscopes always be provided at a location where they can be observed directly.

E. FAULT TREES vs. FMEA'S

Based on DOVAP's conduct of both FMEA's and fault trees for the engine room automation systems, several advantages and disadvantages of both were noted. These are discussed below and DOVAP feels they should be considered if the Coast Guard anticipates requiring one but not both of these types of analyses.

A major disadvantage of fault trees is that they are not accurate without an FMEA to serve as input data. For instance, DOVAP initially prepared the first-cut fault trees before the FMEA's were performed. These fault trees, in general were found unrealistic or incorrect in varying degrees when FMEA results could be considered. Certainly, the top level fault tree events

can be specified without an FMEA, and the second and, perhaps, even the third levels can be identified. However, getting the hardware "plugged into" the fault tree requires data from the FMEA's on the system under consideration.

A potential disadvantage of a fault tree is that it may not cover all the probability. A thorough fault tree will, of course, cover all the probability. It is very easy, however, to overlook certain situations such that certain failures with a distinct probability of occurrence are not included in the fault tree. Also, fault trees may not include the probability of "peripheral failures." For instance, it is seldom possible in a fault tree to list all the items that must be non-failed (power supply, certain supporting functions, etc.). Yet such items have a probability of failure, and contribute to the overall probability of the top level events in the fault tree. It should be noted, however, that including all such items would result in fault trees that were tediously overcomplicated and difficult to follow.

Another disadvantage of fault trees is that for control systems, they can quickly become complicated. Fault trees can model a system in a fairly straighforward manner and without getting overcomplicated. However, when they attempt to model the controls for that system, a second level of detail and abstraction is involved. This quickly introduces additional levels to the fault tree and additional relationships within each level.

The advantage of fault trees lies in their potential for hazard identification. In fact, one of the major advantages of a fault tree is that it is quite good for initial hazard identification. This can be done without going into detailed hardware considerations.

Also, an advantage of a fault tree is that it enables the analyst to find the cut sets and to identify common hardware in different paths. By finding the cut sets, the analyst can determine what type of path exists between hardware failure and critical event. In identifying the common hardware, the analyst can determine where a single hardware item plays a role in more than one critical event.

Another major advantage of fault trees is that they enable the consideration of multiple failures or events. FMEA's, per se, only address single failures or events. Fault trees, on the other hand, through considering possible AND arrangements, can evaluate the potential for a critical event due to two or more failures. In large systems with high failure rates, over a long period of time multiple failures are likely. Therefore, fault trees can serve an important function in analyzing this potential.

Turning to FMEA's, a major disadvantage is if they are done thoroughly, they can be quite costly. Any analytical approach can be costly but the level of detail required to do a thorough FMEA quickly leads to time-consuming expensive analysis.

Another disadvantage is that there is great reluctance to do a thorough job. For reasons that are perhaps understandable, engineers simply do not like to repeatedly consider the effects of part or component failures, and they tend to take short-cuts or simply not consider potential failures.

Another disadvantage of FMEA's, as pointed out in the discussion on fault trees above, is that they can only consider single failures. There is no realistic way that an FMEA can consider multiple failures. For instance, if a system consisted of only two parts, and each of those two parts could either fail open or short, there would be four failure states. As the number of parts increases so does the number of potential failure states. If multiple failures were considered, the number of potential failure states would increase exponentially.

A major advantage of an FMEA is that it forces the engineer to think about failures. This is especially true if the designer performs his own FMEA since then he will become more conscious of the ways his equipment can fail. A related FMEA advantage is that it is the most straightforward technique for involving the designer in reliability considerations.

Other FMEA advantages are generally well known, and in fact involve the reasons for the development and application of the FMEA techniques. These advantages include: (1) FMEA's can provide the most realistic information usually available for reliability modelling and predictions, (2) FMEA's provide a systematic means of evaluating the failure behavior of all hardware within a system, and (3) from the information generated in FMEA's, critical failure modes can be identified and eliminated.

F. WIRING

During the Task II evaluation, DOVAP found that wiring for the systems was adequate. However, on a shipboard automation system evaluated by DOVAP on a previous project, back panel wiring as small as 26 gauge and smaller was utilized. In the potential vibration environment on shipboard, it seems that the wire sizes should be a minimum of 24 gauge. Also, in this potential vibration environment, stranded wire only should be used. ABS automation requirements state that single conductor wire can be used where there is no vibration; however, DOVAP does not feel that vibration can be ruled out for any part of a shipboard automation system.

XIII. GUIDELINES FOR COAST GUARD USE

As part of Task III, the Statement of Work required that DOVAP develop guidelines for use by the Coast Guard in the following areas of its activities:

- Propulsion automation system design approval.
- Accident investigations related to propulsion automation systems.
- Inspections and test of propulsion automation systems.
- Crew training and experience considerations.

The guidelines for each of these areas are provided below.

A. DESIGN APPROVAL GUIDELINES:

The purpose of these recommended guidelines is to provide a workable approach for the design approval of commercial vessel control systems. Due to the limited quantities of systems and components used by commercial vessels, and because cost limitations rule out detailed component qualification and reliability tests, the approach is based on practical considerations necessary for non-military procurements. These recommended guidelines should provide a means for substantially improving life cycle costs and reliability related to automated controls on new vessels.

The basic recommended approach is for the manufacturer, owner/operator, and the shipyard to develop a systems specification which is mutually agreed upon among themselves. The contents of the systems specifications would be provided for by the Coast Guard and would incorporate all aspects of NVIC 1-69* and the following recommended additions and/or modifications. All of NVIC 1-69 will not be repeated in the following recommendations but only those aspects that DOVAP feels should be added or modified. A major source of problems with commercial vessel procurements in the past stems from disagreement between the manufacturers, owners/operators, and shipyards concerning the best approaches for specifying and acquiring automated control systems, and for establishing how to maintain and support the systems once they become operational. By jointly developing a systems specification, these past disagreements should be resolved. Also, the submittal of this systems specification, along with the other data required by NVIC 1-69, will provide the Coast Guard with insights into the configuration of the system

*USCG "Navigation and Vessel Inspection Circular No. 1-69, Subject: Automated Main and Auxiliary Machinery."

and into how the system is to be supported once it is operational.

In order to make valid decisions, with respect to the optimum system design, a historical base is needed. The owner-operator should be concerned with the life-cycle costs of any proposed system. Ths basis for these costs are historical failure rates, maintenance costs, support equipment costs, and other related logistic aspects. DOVAP has found that such historical data is seldom available. In addition to failure rates, the owner/operator needs to know wear-out rates and when equipments should be replaced and/or overhauled.

Many current systems are selected on the basis of the initial cost of the system and on what has been used in the past. Many relatively new systems have not taken advantage of the current state-of-the-art in the electronics field. Again, some of this is due to the lack of historical information which would allow the owners/operators to base decisions on valid trade-off information. In addition to the owners/operators needing data for making logical decisions, the manufacturers and shipyards need data so that unreliable components can be identified and the basic causes of unreliability eliminated. If 100 percent reporting cannot be instituted on all commercial vessels, an alternative plan would be to institute 100 percent reporting on a selected sample of ships. However, DOVAP feels that all vessels with new automated propulsion systems should be required to participate in a data reporting program. If the data system is properly designed, the reporting effort should not appreciably effect the crew's work load.

A.(1) Suggested Systems Specifications Outline:

A.(1)(a) System Concept

In order to ensure the successful application of automated propulsion control systems, the manufacturers, owners/operators, and shipyards should develop a system concept based on acceptable reliability levels and minimum life-cycle costs. As indicated above, many owners/operators base their ideas on equipment that has been used in the past, and do not have historical data for alternative choices. It is suggested that the systems specification contain the results of a preliminary trade-off analysis which considers various system concepts, and justifies the selection made in terms of reliability and life-cycle costs.

Also, many systems are degraded after various operational periods because of poor maintenance practices and wear-out of the equipment. This results in degradation of the initial level of reliability that has been designed into the system, and the system becomes a potential hazard. Therefore, the Coast Guard should not only be concerned with the initial design of the system, but also with how the system is to be maintained

throughout its useful life.

All major aspects of the logistics and support environment should be investigated and form the basis for the support plan. As an alternative to highly trained on-board crew members, the owner/operator should at least consider the possibility of built-in test equipment (BIT) and provide the basis in the system specifications as to why one approach is chosen over the other. In addition, the systems specification should specify other types of support equipment which will be provided on board, such as printed circuit card testers.

Training considerations should cover three levels, that is, the training anticipated of the licensed personnel, unlicensed personnel, and the reliance that is to be put on on-shore personnel. The systems specification should also provide the philosophy as to the number of spares and how spares are to be handled (e.g., storage containers), and the control of limited life items.

A current chronic problem is the lack of adequate maintenance procedures and manuals. The specification should detail the manuals that will be provided, who will generate the procedures described in the manuals, and how they will be maintained and updated.

A.(1)(b) Reliability:

In addition to the system concept discussed above, the systems specification should include anticipated reliability levels for various critical functions. An overall system reliability requirement is not practical because of the many interfaces with manual operations and system overlaps. Therefore, it is suggested that the probability of certain undesirable events occuring be determined, possibly through fault tree analysis. The following preliminary list suggests undesirable faults for steam systems:

a) Loss of low steam pressure alarm.
b) Loss of low steam pressure MPC action.
c) Loss of low steam pressure turbine trip.
d) Loss of boiler level low-low trip.
e) Loss of boiler flame-out trip.
f) Loss of purge fail alarm.
g) Loss of fuel oil low pressure alarm.
h) Loss of feedwater low pressure alarm.
i) Loss of low combustion air alarm.
j) False boiler trip.
k) False turbine trip.
l) Loss of RPM control.
m) Loss of directional control.
n) Loss of turbine control power.
o) Loss of boiler control power.

For Diesel Systems:

a) Loss of abnormal engine shutdown alarm.
b) Loss of abnormal de-clutch alarm.
c) Loss of speed command fail alarm.
d) Loss of direction command fail alarm.
e) Loss of engine safety shut downs (J. W. Temperature high, L.O., Pressure Low, etc.)
f) Failure of station-in-control transfer function.
g) False engine shutdown.
h) False engine de-clutch.
i) Loss of speed control.
j) Loss of direction control.
k) Loss of control system power.

In addition to the quantitative reliability requirements, DOVAP recommends that qualitative reliabiltiy requirements be added to NVIC 1-69, as follows:

Single Point Failures: There should be no single point which would cause the following conditions: open or close fuel oil trip valve; open or close burner valve; insert ignitor; open or close turbine steam valve.

Opens From The Field: Wherever possible, opens from the field should drive the system to a fail safe condition.

Corrosion Prevention: Whenever possible, corrosion resistant parts should be selected.

Power Supplies: Redundant power supplies for boiler controls and turbine controls should be provided, and the supplies should switch-over automatically in case of failure.

Transducers and Sensors: For unmanned engine rooms, there should be redundant sensors for all critical alarms. It is desirable to provide logic that compares the two signals and determines when there is significant difference between the signals indicating that a sensor failure possibility exists. If there is not automatic monitoring of the sensors, the method and frequency for periodically checking the sensors should be stated. Feedback sensors should measure actual positions, not position commands, relative positions of linkages, or intermediate control hardware. Transducers and sensors should be hermetically sealed. Since transmitters used in the field are very susceptible to vibration and heat, precautions should be taken when mounting these instruments. System design should consider sensor accessibility and size.

Switches: No reed switches should be used in field applications. Switches should be hermetically sealed.

Connections and Connectors: There should be sufficient space to make adequate connections. Connectors in the field

should be hermetically sealed.

Pneumatics: Pneumatic system design should include adequate provisions to ensure that supply air is clean. There should be a filter at the final control element.

Circuit Logic: There should be a limited use of potentiometers on printed circuit cards, and also of customizing jumpers. All printed circuit cards should be conformal coated. The design should strive to minimize the number of parts. Series-redundant power input filter capacitors should be provided. The open/close position of valves and actuators should not be determined from timing circuits. Derating policies should be established and stated in the systems specification. Circuit analysis should be performed to establish that the derating criteria has been met. Electrostatic discharge protection should be included in critical circuits. MIL-grade parts should be used for critical circuits.

Alarms: The alarms for critical functions should be initiated from the actual opening and closing of the valve or actuator; alarms should not be initiated solely by circiut logic. Alarms should include all circuit logic that is possible. Therefore, most alarms should receive the initiating signal from just prior to the controller. The following alarms should be added to the list already provided in NVIC 1-69;

Steam Dump Activated.
Low Steam Temperature.
Fuel Oil Pressure High.
Ignitor Extended.

Control Rooms and Control Cabinets: The control room should be cooled to maintain the ambient temperature below 35^{o} degrees C. The control room should be sealed to the extent possible from the external environment to preclude the possibility of fluid seepage from the overhead or deck. Control consoles should have fans for cooling and filters. Control consoles should be mounted on resilient shock vibration dampers.

Wiring: All control wiring should utilize stranded conductors. No wiring should be smaller than 24 gauge.

Throttle Control Hydraulic System: It should be possible to take control within five seconds with the manual back-up for the hydraulic system. If this cannot be accomplished by a handpump, an air pump with an accumulator should be considered.

Boiler Front: High temperature O-rings should be used for all applications. Metal to metal contact with a potential for corrosion should be avoided. There should be direct ventilation on all boiler front equipment. There should be sufficient direct reading gauges on the boiler front for complete manual operations.

A.(1)(c) Component Specifications

The systems specification should contain all individual component specifications, including transducer/sensors, switches, valve operators, valves, pneumatic devices, etc. There are numerous types of sensors for each application and many manufacturers. It appears that the current component selection process is primarily based on cost and on what has previously been used. There is very little data to substantiate whether certain types of components perform better than others, or whether certain manufacturers produce superior components. Apparently the basic method for obtaining sufficient levels of reliability is through warranty agreements lasting from six months to a year. Most current literature provided by component manufacturers contains little, if any, environmental data. Also, very little maintenance or troubleshooting information is provided by these manufacturers. Therefore, to increase the reliability of automated control system components, requirements need to be realistically stated. Also, means must be provided to verify that these requirements have been met.

In order to develop realistic requirements, actual boiler room environments need to be determined. There is considerable conflict between the environmental requirements specified by various organizations such as ABS and IEEE. Also, there is undoubtedly a wide variation from vessel to vessel. Therefore, the spectrum of environments should be determined through measurements on many ships. The actual environmental levels experienced can be provided to the suppliers as design criteria. However, a military type environmental qualification program would be prohibitively costly and probably cause most suppliers to withdraw from the marine field. Also, it has been found on military programs that laboratory testing of one or two items does not actually verify that the component will perform properly in the field environment. That is, the testing of one or two items in a laboratory is not representative of the actual population of parts and environments, and laboratory results are usually better than those experienced in the field.

As previoulsy pointed out, a marine data system would provide information concerning patterns of unreliable part types or manufacturers. Chronic problems could be noted and a problem alert system, such as used by Government Industry Data Environment Program (GIDEP) could be augmented. These alerts could be circulated throughout the marine industry, and manufacturers of substandard components would very quickly be identified.

A.(1)(d) Test Requirements

The systems specification should contain information concerning how the system is to be tested. Because of the high failure rate during the first six months to a year, and the relative inexperience of the crew, it is necessary to eliminate

as many premature failures as possible. This can be accomplished as follows:

Card Burn In: The individual printed circuit cards should be burned-in for a sufficient period of time. Thermal cycling and vibration should be a part of the burn-in process and should be performed on the original equipment and all spares.

Detailed System Testing: Once the system has been installed at tne shipyard, it should be activated and detailed systems testing should be performed. The purpose of this would be to eliminate as many problems caused by shipyard installation as possible, and also to verify operating and maintenance instructions.

A.(1)(e) Workmanship Requirements

Many failures experienced during the lifetime of a vessel are induced by poor workmanship during manufacturing or during assembly and installation at the shipyard. Therefore, the system specificaton should contain provisions for minimizing these problems. It has been found that contamination is a major cause for failure of valves. Contamination can cause valve leakage, sticking of sliding surfaces, increased wear, plugging of small orifices, scoring, and high friction forces. In many cases, sources of the contamination is at vendor or shipyard facilities. Such problems could be reduced significantly if contamination provisions were delineated in the system specification.

A.(1)(f) Electrostatic Discharge

Electrostatic discharge is a problem which is recently receiving increased attention. RCA indicates that ESD accounts for at least 38 percent of the CMOS Semiconductor field failures returned to them for failure analysis. The construction of the current generation of integrated ciruits results in devices which can easily be destroyed or degraded by the discharge of static electricity. To compound the problem, the effects of ESD may produce latent failures which occur sometime during the operational life of the device. Military workmanship specifications and ESD control programs have been published and should be used as guides for this section of the system specification. An ESD program contains the following provisions: it provides for the identification and classification of ESD sensitive components; advises that the contractor and his suppliers exercise ESD protective handling procedures; specifies that technical manuals dealing with all facets of maintenance include caution notices; specifies ESD protective handling procedures; and provides that all ESD sensitve spares be adequately packaged in EDS protective packaging.

A(1)(g) Standardization

Very little standardization exists with respect to marine automation systems because of variations in the type of equipment, and the variety of different components used within the systems. Such lack of standardization creates problems with respect to training individual crew members. It also increases life-cycle costs because of the increased number of spares and types of hardware which must be stocked and supplied. The system specification should include how the manufacturers, owners-operators, and shipyards intend to approach standardization.

B. ACCIDENT INVESTIGATION GUIDELINES:

In addition to the usual data the Coast Guard gathers during an accident investigation (such as general damage to the vessel, operational mode at the time of the accident, time of day etc.), DOVAP recommends that the following questions related specifically to the automated propulsion control system be answered. These questions are general in nature and can be modified according to the specific accident and circumstances.

Questions

- State of the system at time of accident?
- What automated control subsystems were contributing factors to the accident?
- Status of those subsystems at time of accident?
- If the accident was caused by malfunction of one or more propulsion control subsystems, the following questions should be asked to further define the cause of failure;
  - What was the cause of the subsystem failure and what were the symptoms?
  - Was the subsystem failure caused by a faulty component?
  - And if so, what is the class and type of the component?
  - What was the failure mode of the component?
  - Who is the manufacturer of the defective component?
  - Was the failure mode of the defective component verified?
  - Was failure analysis performed on the defective component?
  - What was the conclusion as to the cause of the failure mode?
  - Where is the defective component physically located now?
  - Have similar problems been experienced with these components in the past?
  - Has corrective action been taken to improve the component or obtain a different manufacturer?
  - Is the control system manufacturer and/or shipyard aware of the problems with this component?

- Where was the engine room crew physically located at the time of the accident?
- Where was the chief engineer at the time of the accident?
- What are the names of the crew members on duty at the time of the accident and their classification?
- What is the experience of the crew members on duty?
- What is the training of the crew members on duty?
- How long has this crew been aboard ship?
- Were any abnormalities noted just prior to the accident?
- Were any abnormalities noted in the last 24 hours?
- Were any abnormalities noted in the last six months?
- When was the last time the subsystem was functionally tested
- What was the extent of the test?
- What is the usual frequency for tests?
- When was the subsystem calibrated?
- Is there a preventative maintenance schedule for the failed subsystem?
- When was the last time preventative maintenance was performed on the subsystem?
- Who is the manufacturer of the system and subsystem?
- How many similar systems are currently in operation?
- What is the history of this type of problem as far as the manufacturer is concerned?
- What is the history of this type of problem as far as other owners/operators are concerned?
- Are there other sources that are or should be aware of this problem?
- What is the manufacturer's opinion as to the cause of the problem?
- What alarms, lights, or indicators should have given indications of the problem?
- Were the alarms, lights, and indicators all functioning properly at the time of the accident?
- If there was sufficient indication of an impending problem, what action was taken?
- Why was the action not effective?
- If sufficient warning was not provided, what means could have been provided to initiate a warning?
- Was communication maintained before, during, and after the accident?
- What was the primary means of communications?
- What was the back-up means of communications?

C. INSPECTION AND TEST GUIDELINES:

C.(1) Steam Vessel Considerations

DOVAP feels that periodic Coast Guard inspection and tests should include both a visual inspection of the general conditions of the control systems and the testing of specific items.

C.(1)(a) General Inspections

Control Room. The control room should be checked for general cleanliness and indications of unacceptable maintenance practices.

Engineer's Log. If appropriate, the Engineer's Log should be checked to see if it is complete and current; also problems since the last inspection should be reviewed with the chief engineer.

Control Console. Back panels should be removed from the control console and the following checked:

- Connections; looseness and corrosion.
- Connectors; corrosion and possible loose ends, frayed wires, and contamination.
- Printed circuit boards connector; loose pins, frayed wires, corrosion, and contamination. Check for jury-rigged jumper connections.
- Relay contacts; check for contamination, corrosion, and arcing.
- Filters; check to ensure that they are in place and clean.
- Power supplies; check for signs of overheating and moisture.
- Console lights; check to ensure that all are working.
- Control room horn; check to ensure that all horns are functioning properly.
- Spares areas; check to ensure that the area is clean and that the environment is adequately controlled.
- Spare printed circuit boards; check to ensure that they are packaged and stacked so that they cannot be damaged. Quantities of spare printed circuit boards should be checked to determine if they are adequate.
- Spare piece parts; check packaging to ensure that they are protected from the humidity. Check to determine if the quantities appear to be adequate.
- Limited life items; conditions of piece parts that can deteriorate with age should be checked. Ages of piece parts should be marked. Verify procedures for disposing limited life items when their life has been exceeded, and check stock to ensure that these items have in fact

been removed.
- Filters; check supply of filters to determine if there appears to be an adequate supply.
- Test equipment; check to determine if there are sufficient types and quantities to maintain the vessel. Card tester should be checked to determine if it has been maintained properly.
- Field equipment; check to determine if maintenance appears to be proper. Determine when the field components have been calibrated and time of next anticipated calibration.
- Pneumatic actuators and other devices; check to determine if the air supply is clean, dry, and not contaminated; check drain traps to determine if they have been drained recently.
- Field transducers and switches; check to determine if connections are adequate, check connections and body of sensor for corrosion or other evidence of deterioration.
- Valves; check for signs of leakage, examine body for cracks, leaks, corrosion, etc.

C.(1)(b) Systems Tests

In addition to the general visual inspection of the control room and field components, specific systems tests should be performed. Because of time limitations, all possible tests cannot be run at any one inspection. Therefore, a means should be provided so that the critical functions can be tested. A method for determining the items to be tested based on function criticality and the frequency of failure of the function is provided in the following Table XIII-1. Each of the factors (i.e., criticality and failure frequency) is weighted from 1 to 5, with 5 being the most critical or the most frequent. The total weights are then added and the frequency of the inspection based on the total. The maximum number of points that can be assigned is 10 and the minimum 2. The following overall weighted values indicate priorities that can be assigned to the checkout of an automated propulsion system .

Total Priority Weighting:

9,10; Should be checked each time.
6,7,8; Should be checked at least every other time.
2 - 5; Tested at random as time permits.

TABLE XIII-1
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
1	1st Burner Start Controls	Actuate start boiler firing pushbotton and observe the sequence as described by manufacturer.	5	2	7	4
2	2nd Burner Start Controls	Actuate the second burner-on switch and observe the sequence of events as described by manufacturer.	2	1	3	8
3	Emergency Boiler Trip	Actuate the emergency trip pushbutton. Verify FOTV closes and alarm sounds.	3	5	8	3
4	Forced Draft Fan Failure Causes Boiler Trip	With flame at one burner, stop the forced draft fan. Verify FOTV closes and alarm sounds.	2	4	6	5
5	Drum Hi Water Level Causes Alarm	With flame at one burner, raise drum water level. Verify hi alarm sounds at specified level.	3	4	7	4
6	Drum Lo Water Level Causes Alarm and Lo-Lo Boiler Trip	Lower drum water level. Verify alarm sounds at specified level. Verify FOTV closes at specified level.	4	5	9	2

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
7	Fuel Oil Pressure Low Causes Boiler Trip	With flame at one burner, lower F.O. pressure to burner. Verify FOTV closes at specified value.	4	3	7	4
8	Loss of All Flame Causes Boiler Trip	With flame at one burner, close manual burner oil valve. Verify FOTV closes.	5	5	10	1
9	All Burner Oil Valves Closed Causes Boiler Trip	With flame at all burners. Actuate all burner switches to off. Verify FOTV closes.	4	3	7	4
10	Unsuccessful Burner Shut Down Causes Boiler Trip	With flame at all burners, pin open one burner oil valve and actuate the burner switch for the burner with the pinned valve to off. Verify FOTV closes.	4	3	7	4
11	Loss of Flame Causes Burner Trip	With flame at all burners, close one manual burner valve. Verify that burner oil valve and air register close and burner management problem alarm sounds.	4	3	7	4
12	Loss of Atomizing Steam Causes Burner Trip	With flame at both burners, close one manual atomizing steam shut off valve. Verify that burner oil valve closes and burner management problem alarm sounds.	2	3	5	4

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
13	Burner Oil Valve Not Fully Open Causes Burner Trip	With flame at both burners, disconnect air supply from one burner oil valve to cause valve to be not fully open. Verify that burner oil valve closes and burner management problem alarm sounds.	3	3	6	5
14	Hi/Lo Atomizing Steam Pressure Causes Alarm	Raise atomizing steam pressure and observe that the alarm sounds at prescribed value Lower atomizing steam pressure and observe that the alarm sounds at prescribed value.	2	2	4	3
15	Hi/Lo Fuel Oil Temp. Causes Alarm	Raise fuel oil temperature to prescribed value and observe that the alarm sounds. Lower fuel oil temperature to prescribed value and observe that the alarm sounds.	3	3	6	5
16	High Steam Pressure Causes Boiler Steam to Dump	Raise super heated steam pressure and observe that steam dumps to the main condenser at specified PSI.	5	3	8	3
THROTTLE CONTROL SECTION:						
1	Turning Gear Interlock Functions Properly	Move throttle lever to ahead and astern positions and observe that throttle valves do not open due to turning gear interlock.	2	4	6	5

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
2	Automation of Astern Guarding Valve	With throttle valve at 90 RPM ahead and guarding valve closed, move throttle lever to 40 RPM. Verify that astern guarding valve opens at approximately 55 RPM.	2	5	7	4
3	Guarding Valve Jacked Closed Alarm Activate	With throttle lever at 90 RPM ahead and guarding valve closed, move throttle lever to 40 RPM. Verify that astern guarding valve fail to open alarm sounds. Jack open the astern guarding valve. Verify that astern guarding valve fail to open alarm is silenced.	2	5	7	4
4	Crash Astern Overrides	Move throttle lever to 90 RPM ahead, and when ahead, verify valve is full open, then move throttle lever to crash astern. Verify that ahead valve closes and astern valve opens to 100% within 5 seconds.	5	5	10	1
5	Manual Throttle Trip from Engine Room	Actuate the manual throttle trip. Verify that astern valve closes. Move throttle lever to 60 RPM ahead and verify ahead throttle valve does not open. Reset manual trip, return throttle lever to stop position, depress control reset pushbutton and then move throttle lever ahead and astern. Verfiy that throttle valves respond.	3	4	7	4

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
6	Engine Room to Bridge Transfer	Match bridge throttle lever with the engine room and turn bridge control location switch to bridge. Verify that transfer requested indicating light is illuminated at bridge and engine room. Turn engine room location switch to bridge. Verify that transfer requested lights go out and bridge in control lights are illuminated. Move bridge throttle control lever ahead and astern and verify that throttle valves respond.	3	3	6	5
7	Engine Room May Regain Throttle Control At Any Time	Turn engine room throttle control location switch to engine room and move engine room throttle lever ahead and astern. Verify that transfer requested lights are illuminated, engine room in control lights are illuminated, and throttle valves respond.	3	3	6	5
8	Automation of Guarding Valve and Crash Astern Overrides (Bridge Control)	With throttle lever at 90 RPM ahead, transfer throttle control to the bridge. Move bridge throttle control lever to crash astern. Verify that ahead throttle valve closes, astern guarding valve opens, and astern throttle valve goes 100% open within 5 seconds.	3	3	6	5

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
9	Manual Throttle Trip (Bridge Control)	Actuate the bridge manual control. Verify that astern throttle valve closes. Move bridge throttle lever to 60 RPM ahead. Verify that ahead throttle valve does not open. Reset bridge manual trip and move throttle lever ahead and astern. Verify that throttle valves do not open. Transfer control to the engine room, move throttle lever to the stop position, depress control reset pushbutton, and move throttle lever ahead and astern. Verify that throttle valves respond.	3	3	6	5
10	Low Vacuum Alarm and Lo-Lo Vacuum Throttle Trip	Open ahead throttle to 60 RPM. Lower main condenser vacuum. Verify that low vacuum alarm sounds at specified level. Verify that ahead valve closes at specified level and throttle tripped alarm sounds.	4	5	9	2
11	Lube Oil Gravity Tank Low Level Alarm and Lo-Lo Level Throttle Trip	Open throttle valve to the 60 RPM position. Lower the level in the lube oil gravity tank by stopping the lube oil pump. Verify low level alarm sounds at specified level. Verify that throttle valve closes at specified level and throttle tripped alarm sounds.	4	5	9	2

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
12	Lube Oil Pressure Low Alarm and Lube Oil Pressure Lo-Lo Throttle Trip	Open the throttle valve to the 60 RPM position. Lower the lube oil pressure to the main engine by closing valve at gravity tank. Verify that low pressure alarm sounds at specified level. Verify throttle valve closes at specified level and throttle tripped alarm sounds.	5	5	10	1
13	Low Steam Pressure Alarm and Throttle Run-Back	Open the throttle valve to the 60 RPM position. Lower boiler steam pressure. Verify that low pressure alarm sounds at specified level. Verify that throttle commences to close at specified level. Raise boiler steam pressure and verify that throttle valve opens to its original position.	5	4	9	2
14	Throttle Run-Back Due to Low Steam Drum Water Level	Slowly lower water level in steam drum of one boiler. Verify that throttle commences to close at specified level. Raise water level in steam drum to normal level. Verify that throttle valve opens to its original position.	3	4	7	4
15	Throttle Run-Back Due to High Steam Drum Water Level	Slowly raise water level in steam drum of one boiler. Verify tht throttle commences to close at specified level. Lower water level in steam drum to normal level and verify that throttle valve opens to its original position.	5	4	9	2

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
AUXILIARY SECTION:						
1	Automatic Start of Standby Lube Oil Pump	With one main lube oil pump in service and the other on standby, stop the in-service pump. When discharge pressure of in-service pump drops to the specified PSI, the standby pump starts and the in-service pump failure alarm sounds.	4	5	9	2
2	Automatic Start of Standby Main Feed Pump	With one main feed pump in service and the other on standby, stop the in-service pump. When discharge pressure of in-service pump drops to the specified PSI, the standby pump starts and the in-service pump failure alarm sounds.	4	5	9	2
3	Low Control Air Alarm	Lower control air pressure and observe that that alarm sounds at specified PSI.	2	5	7	4
4	Deaerator Level Alarm	Lower deaerator water level and observe that the alarm sounds at specified level. Raise deaerator water level and observe that the alarm sounds at specified level.	2	5	7	4
5	Atmospheric Drain Tank Level Alarm	Raise atmospheric drain tank water level and observe that the alarm sounds at specified level. Lower atmospheric drain tank water level and observe that the alarm sounds at specified level.	4	4	8	3

TABLE XIII-1 (cont)
RECOMMENDED PRIORITIES FOR OPERATIONAL TESTS OF THE AUTOMATION SYSTEMS FOR STEAM TURBINE SYSTEMS

STEP	OBJECTIVE	PROCEDURE	Likelihood of failure 1-5 5 highest	Criticality (5 most critical)	Total Weight	Priority Ranking
6	Bilge Level Alarm	Activate each engine room bilge well high level alarm.	3	5	8	3
7	Loss of Power Supply Alarm	Secure power to control console and observe that alarm sounds.	2	5	7	4
8	Lube Oil Pressure Alarm	Lower lube oil pressue on each SSTG and observe that alarm sounds at specified level.	3	5	8	3

C.(2) Diesel Vessel Inspection Considerations

As pointed out in the fault tree discussions, the vast majority of diesel automation system failures that can cause an undesirable event have no means for manual intervention. This is also borne out in the criticality analysis. This occurs on the diesel system evaluated during this study for two reasons. First, there are no "pipeline processes", as discussed earlier, so that when a failure occurs it will "take effect" immediately. Second, most alarms and trips are provided to prevent machinery damage (for instance, from low lube oil pressure, high jacket water temperature, etc.)

These failure characteristics significantly limit the possible approaches for safety inspections. Alarms and trips can, and should be, tested although in many cases an "end to end" test will not be possible. Such an "end to end" test would verify proper operation of all elements from initiating sensor to final audible and visible alarm. On a steam vessel, for instance, such an end to end test on the drum level alarms can be performed by changing the drum level. On a diesel vessel, on the other hand, one would not want to lower the lube oil pressure, raise the jacket water temperature, etc. Instead, such alarms would have to be tested by stimulating the sensor in some manner dependent upon the specific sensor.

From a safety standpoint, a more significant type of inspection would involve verifying that all operational modes were non-failed. On the diesel vessel evaluated during this study, several operating modes, and combinations thereof, were provided (e.g., bridge in control, engine room in control; cruise mode, maneuver mode; one-engine modes, two engine mode.) Some of these modes, and combinations of modes, will be utilized infrequently. Therefore, failures effecting them might not be detected until that particular mode/mode combination is needed. Such failures can include loss of ability to go astern, uncommanded speed changes, etc., and had one of these failures occurred, it would "take effect" instantaneously when the effected operating mode was selected. Periodic inspections of all operating modes and combinations of modes would provide some assurance that failures would not go undetected.

D. GUIDELINES FOR CREW TRAINING AND EXPERIENCE CONSIDERATIONS

D.(1) Training and Experience Factors

When evaluating training requirements for crew members who operate and maintain automated propulsion systems, many factors have to be considered. These factors are interrelated and are as follows.

a) Type of System:
The type and extent of the training has to be considered in terms of control system complexity and the state of the art of the system.

b) The Level of Sophistication in Built-In Tests:
Increased capability of the BIT reduces training requirements of crew members in the areas of operational testing and fault isolation. The level of BIT must be traded off to determine the cost benefit versus the degradation in reliability due to the additional equipment. Also, the initial cost of the additional BIT equipment must be considered.

c) Better Availability of On-Shore Personnel:
If on-shore personnel were available to perform scheduled and non-scheduled maintenance, the need for highly trained crew members would be reduced.

d) Ability of Back-Up Systems to Take Over the Load:
If the primary systems could be out of operation for extended periods of time, with no hazard to vessel navigation, the need for immediate diagnostics and repairs would be minimized, thus also minimizing the need for crew members to perform these functions.

During the evaluation of training requirements, much information was obtained from Log Number 600, entitled, "An Assessment of Shipboard Sensors and Instrumentation." In the study reported in this document, extensive interviews were conducted with owners/operators of U.S. flag ships, ship builders and manufacturers of automated control systems. Also, foreign owners/operators and manufacturers were interviewed. In addition, a great deal of information was obtained during the on-board observations of Vessels A and B, made by DOVAP, and from the interviews with the chief engineers. During this study, DOVAP was assisted by two automation repair firms

and their opinions were also obtained concerning training level requirements.

One of the major problems related to training is that generally the crew does not understand reliability and how various environmental factors and preventative maintenance affect the long-term reliability of the control system. As examples, DOVAP personnel observed one control system being operated without the back panel on the control console. Also, it was observed that the filters had been removed from the control console. It appears to DOVAP that by operating the control consoles in this manner, the crew does not understand why the cabinets are enclosed and the effects on the circuit cards of not keeping them closed. One failure mode that is very difficult to isolate is due to contamination of printed circuit card connectors. The probability of this failure mode is increased when the filters and/or back panels are removed.

At the current time, the USCG sets the standards for both licensed and unlicensed crew members. The Coast Guard also certifies applicants who have met the standard requirements and passed the certification test. However, the certification tests do not currently require knowledge of automated control systems. There are various schools that offer preparation for the USCG certification. Here again, these schools do not provide adequate training on automated control systems.

A typical example of the experience of licensed crew members involves Ship B. The chief engineer had considerable experience with automated control systems and had attended various manufacturers' schools. The first assistant had 35 years of experience in all types of ships and had worked on automated APL and LNG ships. He had also been through a variety of schools. The second assistant and third assistant engineers were both fairly "green" with limited experience in automated propulsion controls. On this ship, the chief engineer performs all troubleshooting and is in the control room during maneuvering and start-up.

Some owners/operators, and shipyard personnel report that equipment is being poorly maintained, and that this neglect is a major cause of system malfunctions. It is also generally felt that the systems are becoming too complex for one operating engineer to understand, and that improved diagnostic techniques are needed. Shipyards usually provide training for new systems and some claim that the owners/operators are not taking advantage of the shipyard-offered courses. Shipyards also claim that feedback from the owners/operators is not sufficient.

The need for a better data collection system was discussed previously. If chronic problems are going to be isolated and resolved, they must be documented. Manufacturers and shipyards

must be aware of the problems in order for corrective action to be taken. The manufacturers generally provide in-plant training and documentation and also have personnel aboard during sea trials to train the crew and perform final check-out of the system. Training is the most critical during the first year of vessel operation. During this time, the new system being put into service will contain many manufacturing and shipyard induced problems. The failure rates will be anywhere from three to eleven times higher than during normal steady state operations. Also, during this time, a relatively "green" crew will be taking over the system, trying to isolate failures as they occur and also become familiar with the system.

Most owners/operators report that union training programs do not provide the type of training needed for maintaining automated control systems. Also, there is no set schedule for upgrading personnel capabilities. One important factor that must be considered when specifying new control systems is that the design of the system should not be limited to the current capabilities and skill levels of crew members. There is a tendency for some owners/operators to remain with pneumatic controls even though electronic systems are probably more reliable and require less maintenance. Part of the basis for this selection is that the crew generally understands pneumatics, whereas electronics, in most cases, is foreign to their current capabilities.

D.(2) Automation Personnel

Training can generally be broken down into three categories, that is, (1) unlicensed crew members, (2) licensed crew members, and (3) shoreside personnel. The availability and capabiity of the three are interactive, and training levels of one affect the required levels of other groups.

The following are DOVAP's recommendations for the three levels of capabilities. However, these recommendations must be modified based on the operational scenario, type of diagnostics available, type of equipment, adequacy of manuals and other documentations, and size of the operator's fleet.

AUTOMATION ENGINEER SPECIALIST:

It would be desirable to have one permanent engineer onboard at all times who has been especially trained for troubleshooting, servicing, and maintaining the automated control system. He would be on hand for all critical maintenance actions and troubleshooting. He should have attended the manufacturer's training school. It would be helpful if he attended training sessions or had been on-board during sea trials. He should have a background in the technoloy used to implement the system (e.g. electronics).

OTHER AUTOMATION SYSTEM CREW MEMBERS:

The other crew members should have had training in general types of control systems. Because of frequent switching from vessel to vessel, it is not practical to train all of the crew members in specific systems. As pointed out previously, crew members would be indoctrinated into the fundamentals of reliability and environmental effects on certain components. Training of these crew members should be such that they are familiar with circuit logic and circuit schematics. The function of these crew members should be limited to routine operation of the control systems and in assisting the automation specialist in the isolation of problem areas and during calibration of the system.

When a malfunction on-board occurs, the immediate problem is to restore the system to normal operation or a satisfactory level of reduced performance. This usually entails the activation of one or more back-up systems. Because there is always a possibility of the back-up system not functioning properly or eventually failing, it is desirable to troubleshoot the original system and repair it as soon as possible. In addition to training, various aids could assist in the isolation of failures and expedite restoration of the system to the proper performance levels. As mentioned before, upgraded maintenance manuals and diagnostic procedures would assist in the isolation of problems. Also, computer-aided diagnostic routines would greatly facilitate the isolation of problems, especially in digital circuitry. Small mini-computers could be located in the control room with software routines for diagnostics of specific problems. The software logic would determine checkpoints and the most direct route for isolating problem areas. As previously discussed, the Ship B burner master module contains 42 digital circuit cards. If a fault occurred in this digital system and the engineer tried to fault isolate by randomly replacing cards, restoration of the system could be a very time-consuming task.

SHORESIDE PERSONNEL:

Shoreside personnel fall into three categories: (1) manufacturer's representatives; (2) highly skilled automation system repair independent service companies; (3) on-shore pools of personnel maintained by large shipping companies. Most owners-operators utilize the service of on-shore personnel for more complex problems. The biggest problem is the availability of these people when needed, and the turn-around time for restoring the equipment to normal status. On-shore personnel are also utilized for system calibration, a very time-consuming task which is usually required from every six months to every twelve

months. Some vessels with complex control systems utilize on-shore personnel on the average of once a month. The training of the on-shore personnel does not fall within the realm of training requirements; however, the availability and capability of these people must be kept in mind when considering training requirements for on-board crew members.

D.(3) Additional Comments

As discussed above, training requirements can be reduced through the provision of built-in test (BIT) and on-board circuit card testers. However, there will likely be control system areas that such test provisions will not cover. A major area would be relays that are not mounted on printed circuit cards, and are therefore not testable via the card tester. On Ship A, such non-card mounted relays are used extensively for feedwater control and burner demand sequencing. Failure of such relays would be extremely difficult to troubleshoot without some type of signal tracing and knowledge of what the signals were supposed "to be doing."

When control systems include such areas, it would be desirable for at least one crew member to be trained in the use of wiring diagrams for signal tracing, and in the use of appropriate signal tracing instruments. In some cases, signal tracing could be accomplished with a multimeter, but more likely an oscilloscope would be required.

XIV. CONCLUSIONS AND RECOMMENDATIONS

During the Task I literature review, a wide variety of topics related to automated propulsion systems were reviewed. Generally the discussions in the literature were of a qualitative nature. Some quantitative data was given, but in many cases the basis for the data was not fully explained. The general conclusions reached from the literature reviews are as follows:

a) The reliability of commercial vessel automated propulsion systems needs improvements;

b) No formal reliability efforts related to design are currently applied by United States manufacturers;

c) When discussing individual problem areas, most papers state that sensors are problems but give no positive suggestions for improvement;

d) Component are selected primarily on the basis of cost, unless component provisions are specifically stated in the design criteria;

e) It is generally agreed that automated propulsion systems for commercial vessels should be better supported with improved training, improved manuals and documentation, and better spares and preventative maintenance programs;

f) Standard environmental criteria needs to be defined and;

g) A commercial vessel failure data system needs to be established.

In reviewing all literature sources, certain subjects were conspicuous by their absence. These are:

a) No formal reliability evaluations of commercial vessel systems were reported;

b) No cost effectiveness studies of current propulsion systems were reported.

The general theme reflected in all of the documentation is that there is a need to improve the reliability of current automated propulsion systems. However, few facts were given to support these conclusions, and in most cases, means for accomplishing these were vague or not discussed at all. In reviewing these papers, DOVAP noted that the authors had a tendency to

imply that either the equipment was not specified correctly, or that it was not supported correctly once it became operational. Manufacturers tended to claim that the shipyard environment degraded the equipment, and again that it was not supported correctly when it became operational. It is apparent from reviewing this literature and from discussions with manufacturers, owners/operators, and shipyard engineering personnel, that a means is needed to get all involved to work together in order to design, install, and operate systems in a manner that will ensure adequate reliability.

The major part of Task II consisted of a reliability analysis of three typical vessels. These included two steam vessels, designated Ship A and Ship B, and one diesel, designated Ship C. The reliability analysis included a) reliability predictions, b) failure modes and effects analyses (FMEA), c) criticality analyses, and d) fault tree analyses. While all four of these analyses fall under the general category of reliability and safety analysis, they are basically different and produce different results. However, all of the analyses are interrelated, and some provide inputs to the other analyses. As an example, the basis for all of the analyses consists of the basic failure rates. For the failure rate predictions, five categories of rates were generated, namely:

a) Basic Failure Rates; The basic rates are for a ship-sheltered environment (i.e., on a ship but not on deck), and an ambient temperature of 35 degrees C, and are based on the use of commercial grade parts, the steady state period of the operational life of the vessel, and on no scheduled or preventative maintenance.

b) Temperature Effect Failure Rates; This failure rate is for all of the same conditions as for basic failure rates except that the temperature is changed from 35 to 50 degrees C.

c) Failure Rates For Improved Quality Levels; These failure rates are the result of changing the part quality levels from commercial grade to the lower military grade parts.

d) Premature Failure Rates; These convert the failure rates for the steady state period to those of the infant mortality, or premature period. This premature period usually lasts from initial system operation through approximately the first six months of system life.

e) Failure Rates For Maintenance Improvements; These failure rates reflect the improvement in the basic failure rate occurring from a comprehensive preventative maintenance program.

The Failure Mode and Effects Analysis (FMEA) utilizes the basic part failure rates. These failure rates are subdivided to cover the failure modes for specific parts, and the modes are then evaluated to determine the effect of the failure on the next higher assembly and the subsystem. The FMEA did not consider system criticality or redundancy, nor the effects of any of the adjustment factors.

The criticality analysis utilized the results of the FMEA to determine the consequence of each failure. The end effects were estimated based on the most probable series of events. The criticality analysis also evaluated the effect of the four factors.

The Fault Tree analysis provides the most precise estimate of any undesired condition. It is a probabilistic analysis, and depicts all events that could contribute to undesirable events. Because of the complexity of this analysis, usually only a few top undesirable events are selected and analyzed. It would not be economically feasible to evaluate the probabilities of all events.

A. RESULTS OF PREDICTIONS.

The overall basic failure rate predictions for the three ships are as follows:

	Basic Failure Rate	Mean Time Between Failure
Ship A	.007988	125.2 hours
Ship B	.003622	276.1 hours
Ship C	.001015	984.9 hours

As previously discussed, the basic failure rate is that which would be experienced with no scheduled or preventative maintenance. That is, each component is allowed to degrade until it eventually becomes a functional failure. However, even if the component does degrade until it becomes a functional failure, the failure may not have a critical effect on the system. Examples of such failures are those which cause loss of alarms or backup equipment.

The highest predicted failure rate for the three systems evaluated is for Ship A, which averages approximately 5.8 predicted failures per month. The principal reason for the difference between the two steam vessels is that Ship A's automated propulsion system is more complex than Ship B's. Ship A, also, has three burners per boiler, while Ship B has two. Ship A, also, has provisions for automatically sequencing the burners on and off. Also, Ship A contains a great deal of pneumatic

equipment which has a relatively high failure rate. Ship C is the diesel vessel and its control system is not comparable to those of the steam systems, which are much more complicated.

It is predicted that Ship B will average approximately 2.6 failures per month.

As previously discussed, the failure rates can be reduced by approximately 50 percent through a comprehensive preventative maintenance program. If this were instituted and the basic failure rates were reduced by half, the expected number of failures per month for Ship B would then be 1.3. This prediction of 1.3 failures per month is close to the 1.6 failures per month derived from the Navy 3M data system for the actual occurrence of Navy propulsion system failures. This gives a good substantiation for the predicted values, since the Navy does have comprehensive preventative maintenance programs.

As previously indicated, these failure rates can be adjusted either upwards or downwards by the various factors. For instance, increasing the temperature increases the failure rates by approximately 22 percent; quality improvements through the use of military grade parts decreases the failure rates by 53 percent; shifting from the steady state to the premature operational phase increases the failure rates by a magnitude of 6.

Some quantitative data obtained during Task I provides comparative frequencies. As an example, one report summarizes findings concerning the frequency of alarms from 20 ship-years of accumulated history. This paper reports that on average, turbine tankers experienced 3.5 alarms per month. This is relatively close to the 2.6 failures that are predicted for Ship B, although failures cannot be directly compared to alarms. The number of failures should be somewhat less than the number of alarms because some alarms result from components' parameters drifting or calibration problems, and only require adjustment.

B. FAILURE MODES AND EFFECTS ANALYSIS.

The FMEAs revealed conditions that are contrary to good reliability practices. Some of these are as follows:

a) Excessive use of components;

b) Use of a single sensor for both an alarm and a function signal used in the control logic;

c) Extensive use of low quality grade components;

d) Lack of electro-static discharge protection;

e) Use of logic configurations that introduce either undesirable failure modes, per se, or an increased number of undesirable failure modes.

Specific situations illustrating the above situations are discussed in a "case history" format in Section X.

C. CRITICALITY ANALYSIS.

In order to evaluate the criticality associated with each failure mode, a criticality analysis was performed. Due to the complexity of the analysis and the fact that the basic results were the same for Ships A and B, only Ship B was analyzed quantitatively. The total predicted failure rate for Ship B, using the basic rates, was 0.003627 failures per hour, or a mean time between a failure of 276.1 hours. Using a normal cruising time of 710 hours, the expected number of failures per normal cruise is 2.57. Figure XIV-1 is a criticality analysis printout which shows the distribution of the 2.57 failures arranged in order of mission criticality. These are expected frequencies for normal cruising.

During the normal cruising period, permanent damage to either the boiler or turbine is ranked first in terms of criticality, and temporarily reduced RPMs is third. The most frequent mission effect is small performance degradation, which accounts for 23 percent of the total failures. Twenty-three percent of the expected total number of failures per cruise results in an average of 0.6 times per cruise when a failure would cause a small performance degradation. Because "small performance degradation" is rather inconsequential during normal cruising, the mission loss probability is computed as 0.1. Therefore, even though the classification of the mission effect of "small performance degradation" is highest by frequency, because of the low mission loss probability it is ranked 5th in terms of it's contribution to mission criticality.

The number one ranked mission effect, possible boiler or turbine damage, accounts for a probability of 0.48, with a percentage contribution to the total criticality of 35 percent. This mission effect has to be discounted to some extent however. The possible boiler damage is due to either possible steam or combustion explosions, and turbine damage is due to such possible problems as high drum level or wet steam. This mission effect is nebulous because the true probabilities of occurrences are influenced by factors external to the propulsion control system, and usually damage is not instantaneous. Turbine damage usually results from the effects of repetitive failures over time, or from one condition being allowed to exist too long. These cumulative types of damage factors could not be evaluated during this analysis.

MISSION EFFECT CRITICALITY

MISSION EFFECT	NO.	SYSTEM EFFECT FAILURE PROBABILITY	PCT. OF SYSTEM FAILURE PROBABILITY	MISSION LOSS PROBABILITY	MISSION CRITICALITY	PERCENT CONTRIBUTION TO MISSION CRITICALITY
7 POSSIBLE BLR/TURB DAMAGE	1	.4806	18.53	.5000	.2366	35.44
12 TEMPORARY LOSS OF RPM CONTROL	2	.2475	9.540	.6000	.1437	21.52
5 TEMPORARY REDUCED RPMS	3	.2896	11.16	.4000	.1147	17.19
10 TEMPORARY DIM	4	.9220E-01	3.554	.7000	.6393E-01	9.584
3 SMALL PERFORMANCE DEGRADATION	5	.6034	23.26	.1000	.5951E-01	8.914
13 TEMP LOSS DIRECTIONAL CONTROL	6	.8640E-01	1.789	.6000	.2735E-01	4.096
14 BACK-UP FAILURE	7	.1095	4.219	.2000	.2173E-01	3.254
2 NO EFFECT	12	.2303	8.877	.0	.0	.0
1 NOT APPLICABLE/NORMAL STEAMING	14	.4948	19.07	.0	.0	.0

FIGURE XIV-1

Mission Effect Summary, Basic Failure Rates,
Normal Steaming Phase

Therefore, discounting the number one mission effect, the remaining top three mission effects account for 24.7 percent of the expected failure rate for normal cruising. This amounts to a failure rate of 0.63 for the remaining top three events, or mean time between occurrence of 1120 hours. This is equivalent to a relatively serious problem occurring on average 7.6 times a year during normal cruising. The expected frequency of temporarily reduced RPMs, the number three ranked mission effect, is 0.29 per cruise. This gives an expected rate per year of 3.4. This compares almost exactly to one report reviewed during Task I which documents 41 ship-years of history and reports a slowdown rate of 3.3 per ship-year.

D. FAULT TREE ANALYSIS.

Of the four analysis techniques, the Fault Trees are the most precise. The failure mode probabilities were based on the exponential distribution and are computed for one cruise of one-month duration. Each probability of occurrence was computed twice, once with the probability of manual intervention being effective 90 percent of the time (or, noneffective 10 percent of the time), and once with no manual intervention. Noneffective manual intervention could be due to an alarm failure, incorrect action taken by the crew, action not timely enough to prevent problems, etc. The probability of alarm failure is relatively small, in most cases less than 5 failures per one-million hours. This probability can also be significantly reduced by periodic testing of alarms. The probabilities do not take into account such backups to alarms as indicators, lights, and other gages.

In calculating the probabilities of the top level undesirable events, all possibilities had to be considered. Examination of some of the branches of a fault tree will indicate relatively high probabilities of occurrences at the bottom of the tree. However, due to "AND" logic where two or more events must occur for the upper event to occur, some of the probabilities become insignificant.

Table XIV-1 summarizes some of the probabilities of the top level undesirable events for the two steam systems, and gives the probabilities with manual intervention being 90 percent effective (or 10 percent noneffective) and with no manual intervention. One of the top undesirable events is unscheduled turbine shutdown. The probability that Ship A will experience an unscheduled turbine shutdown when manual intervention is 90 percent effective during a cruise is 0.1584; this probability for Ship B is 0.1065. This amounts to approximately 1.9 such shutdowns per year for Ship A and 1.27 for Ship B. As expected, the probabilities increase significantly with no manual intervention; for Ship A the probability increases to 0.5186 and for

TABLE XIV-1

Probability Of Undesirable Events Occurring
Probabilities Per Cruise (730 Hrs) and
Expected No. Per Year, Ships A and B

	Assuming a 90% Correct Manual Intervention				No Manual Intervention	
	Ship A *	No. Per Year	Ship B *	No. Per Year	Ship A *	Ship B *
1. Unscheduled Turbine Shutdown	0.1584	1.90	0.1065	1.27	0.5186	0.2861
a) Combustion Explosion	0.0180	0.21	0.0143	0.17	0.0297	0.0522
b) Steam Explosion	0.00014	0.002	0.0046	0.055	1.42×10^{-4}	0.0451
c) Single Boiler Trip	0.1244	1.49	0.0446	0.54	0.2040	0.0606
d) Both Boilers Trip Due To A Common Cause	0.0392	0.47	0.004	0.005	0.1986	0.0131
2. Turbine Damage	0.0358	0.42	0.0392	0.47	0.1026	0.1360
3. Loss of Space/Directional Control	1.1×10^{-6}	-	1.1×10^{-6}	-	-	-
a) Loss of Primary TC**	0.1682	2.02	0.1682	2.02	-	-
b) Loss of Hand Pump	0.0246	0.29	0.0246	0.29	-	-
c) Loss of Handwheel	0.0027	0.03	0.0027	0.03	-	-

(*Probability)
(**Throttle Control)

Ship B to 0.2861.

The 1.9 and 1.27 predicted stoppages at sea compares closely with information given in a paper that documents the history of 29 tankers. This paper reports an average stoppage at sea rate of one per ship per year. The results of the DOVAP study are slightly on the pessimistic side, mainly because it was necessary to estimate the frequencies of certain occurrences outside of the automated propulsion system itself. In some cases, it was assumed that such occurrences had either a hundred percent or a very high probability of occurrence. The subevents under unscheduled turbine shutdown in Table XIV-1 are given to show some of the relative probabilities; it should be noted, however, that these are not additive. As an example, both boilers must fail in order for an unscheduled turbine shutdown to occur. The frequency of boiler trips for Ship B is predicted to be 0.54 per year. As a comparison to actual historical data, one report which was reviewed during Task I reported 0.45 trips per year based upon 62 ship-years of history.

The probability of explosion, either combustion or steam, is 0.0181 for Ship A and 0.0189 for Ship B. This amounts to an estimated mean time between explosions of 33,000 hours for Ship A and 37,000 for Ship B. As a comparison, it was estimated from two sources of historical data that explosions occur once every 36,000 hours in steam systems. Therefore, the estimates for Ship A and Ship B are relatively close to the data reported from historical analysis.

The probability of a single boiler trip is substantially higher for Ship A than Ship B. This is to be expected because Ship A is more complex and also utilizes a considerable amount of pneumatics which have higher failure rates than electronics. The total effect on the unscheduled turbine shutdown probability, however, is not that significant since the probability that both boilers are down simultaneously reduces the difference. Turbine damage was not included in unscheduled turbine shutdown. This is because, as previously explained, turbine damage calculations are nebulous.

The top undesirable event of loss of speed/directional control becomes very inconsequential. As can be seen, the probability of loss of the primary throttle control mode, with a probability of 0.1682 per cruise, is relatively high. However, double redundancy is provided by the hand pump and the hand wheels, so probability of losing all control modes becomes extremely small.

The top event for the diesel system fault tree is "vessel does not respond as commanded due to engine room automation faults." The probability of this top event is 0.072, or roughly 0.9 occurrences per year.

E. OVERALL CONCLUSIONS AND RECOMMENDATIONS.

Based on the values predicted by DOVAP and the data from the literature search, it is felt that the automated propulsion systems analyzed during this study have acceptable levels of reliability. However, it must be noted that this applies to the conditions considered during the study analyses. If a specific vessel spends a great deal of time maneuvering and in close quarters, the reliability of the propulsion automation system must be substantially higher. With the current level of technology, reliability of commerical vessel automated propulsion systems could be magnitudes higher. Such higher levels of reliabilities have been achieved in the aerospace industry. However, any increase in reliability also entails an increase in cost. Also, it should be noted that there is not a one to one ratio between improvements in reliability and relative increases in cost. As increasingly higher levels of reliability are sought, the ratio of cost to reliability increases. It should additionally be noted that increased reliability does not necessarily decrease maintenance costs. On the contrary, increased reliability often results in increased complexity which can have the net effect of increasing maintenance costs. Again, in the military environment, equipment currently in use displays magnitudes higher achieved reliability levels as compared to commercial automation propulsion systems. The military are also consuming a large percentage of their total budget in maintaining these systems.

Section X, Reliability Design and Performance Criteria, discusses ways in which the reliability of commerical vessel automated propulsion systems can be increased. Most of these suggestions will increase the cost of the propulsion systems. As an example, changing from commercial quality grade electronic components to the higher quality level grades would substantially increase both reliability and costs. Therefore, in order to design, install, and support any new automated propulsion system, all requirements of proposed systems should be predefined and cost trade-offs considered. DOVAP recommends that a system specification be generated jointly by the control system manufacturer, the shipyard, and the owner/operator. The system specification should provide the desired levels of reliability for critical functions, and specify how the desired levels are to be achieved. The system specification should also define how the system is to be supported during its operational life. During support considerations, trade-off evaluations should include the pros and cons of Built-In Test (BIT) versus manual test and fault isolation.

In the area of support for operational equipment, the system specification should specify the levels of training required for the various crew members. DOVAP suggests that at least one member of the crew be trained as a propulsion system control

specialist. This member need not be the chief engineer, but the chief should be on hand during critical maneuvering operations. He also should be the principal investigator in the trouble shooting and corrective action of the automated propulsion system. Also, required levels of manning for the control room should be specified in the system specification. If periods of unmanned engine room operation are planned, alarm provisions should be adequate, and certain critical alarms should be redundant. The systems specification should also delineate how the system is to be manned during the first 6 months when failure rates could be up to six times greater than during the steady state period of the operational life. Additionally, the system specification should contain provisions for minimizing this period through workmanship requirements to reduce manufacturing induced problems. It should contain details on the tests to be conducted during sea trials, and specify the training of the crew that will be necessary prior to sea trials. The systems specifications should also describe in detail the preventative maintenance plan that will be applied during the operational life of the system, including how components which are subject to degradation or wearout are to be periodically replaced or overhauled.

DOVAP's last recommedation is that a data system for the collection of failure related information be established. Throughout the entire study, it was obvious that many of the opinions expressed in the literature and in personal contact were based on observations that can easily be influenced by recent occurrences or by emotional factors. In order to reduce such subjective biases, and provide objective means for evaluating reliability and costs, component failure rates, maintenance requirements and approaches, and other reliabilty-related factors, a historical data base is very much needed.