

AD-A190 285



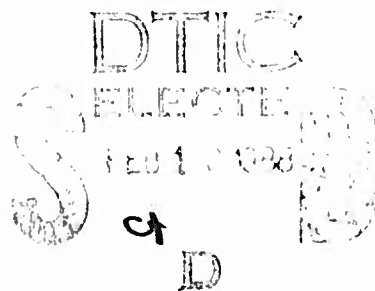
THE FILE COPY

1801 RANDOLPH ROAD, S.E. ALBUQUERQUE, NEW MEXICO 87106 (505) 848-5000 TWX 910-989-0619

Software Supportability Risk Assessment in OT&E: Measures for a Risk Assessment Model

FINAL

DISTRIBUTION: UNLIMITED



SEPTEMBER 28, 1984

BDM/A-84-565-TR

88 2 04 018



September 28, 1984

DISTRIBUTION: UNLIMITED



A-1

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

H.D. 21175 2-5

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified			1b. RESTRICTIVE MARKINGS None	
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION/AVAILABILITY OF REPORT Unlimited	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE				
4. PERFORMING ORGANIZATION REPORT NUMBER(S) BDM/A-84-565-TR			5. MONITORING ORGANIZATION REPORT NUMBER(S)	
6a. NAME OF PERFORMING ORGANIZATION The BDM Corporation		8b. OFFICE SYMBOL (If applicable)		7a. NAME OF MONITORING ORGANIZATION Air Force Operational Test and Evaluation Center/RMC
6c. ADDRESS (City, State and ZIP Code) 1801 Randolph Rd., SE Albuquerque, NM 87106			7b. ADDRESS (City, State and ZIP Code) Kirtland Air Force Base, NM 87117	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Same as 7a		8b. OFFICE SYMBOL (If applicable)		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER F29601-80-0035/SS304
8c. ADDRESS (City, State and ZIP Code) Same as 7b			10. SOURCE OF FUNDING NOS.	
			PROGRAM ELEMENT NO.	PROJECT NO.
			TASK NO.	WORK UNIT NO.
11. TITLE (Include Security Classification) Software Supportability Risk Assessment in OT&E:				
12. PERSONAL AUTHOR(S) W. Huebner, D. Peercy, G. Richardson				
13a. TYPE OF REPORT Technical		13b. TIME COVERED FROM 4/16/84 TO 9/28/84		14. DATE OF REPORT (Yr., Mo., Day) Sept 28, 1984
15. PAGE COUNT 75				
16. SUPPLEMENTARY NOTATION				
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUB. GR		
19. ABSTRACT (Continue on reverse if necessary and identify by block number) Assessing the software supportability risk of Air Force acquired systems is necessary to enable various decision makers to properly plan for system deployment. Risk assessment (RA) is required throughout the system acquisition life cycle. Since the perspective of OT&E is focused upon the overall system mission, including supportability, methods are required which provide software testers with areas which require testing emphasis and which provide decision makers with an assessment of software and software support risk for production decisions. Due to the complexity of these requirements, it is necessary to determine the feasibility of developing and implementing a risk assessment model of software supportability with the proper system mission perspective to ultimately assist the top level decision maker. This report contains the results of an analysis of candidate measures of software supportability to determine the level of effort and usefulness of developing and implementing a risk assessment model for software supportability (RAMSS) in OT&E. (SEE NEXT PAGE)				
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☒ OTIC USERS ☐			21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Major Gary R. Horlbeck			22b. TELEPHONE NUMBER (Include Area Code) 505-846-1254	22c. OFFICE SYMBOL LG5T

portion of this document.
Item 11 (cont'd):

Measures for a Risk Assessment Model (FINAL).

Item 19:

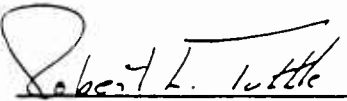
The document also describes the model framework and assesses the feasibility of model development and implementation under this framework.

FOREWORD

This technical report, BDM/A-84-565-TR, is submitted by The BDM Corporation, 1801 Randolph Road, S.E., Albuquerque, New Mexico, 87106, to the Air Force Operational Test and Evaluation Center, Kirtland Air Force Base, New Mexico, 87117. This report is in compliance with CDRL item A008, Contract F29601-80-C-0035, and fulfills the requirements of paragraph 7.5 of Subtask Statement 304/00, titled "Software Risk Assessment in OT&E," as amended by Subtask Statement 304/01, /02, and /03.

This report was the result of effort by Mr. Walter Huebner, Jr. (Task Leader), Dr. David Peercy, and Dr. G. Don Richardson of The BDM Corporation. The primary Subtask Statement Project Officer was Maj. Gary R. Horlbeck (AFOTEC/LG5T); the alternate Subtask Statement Project Officer was Mr. Jim Baca (AFOTEC/LG5).

Reviewed by:


for Fred A. Ragland
Program Manager

PREFACE

The use of the term "ADP" or "system" in this document is not meant to imply any particular functional category or system. In particular, the term is meant to encompass at least the four categories outlined in AFR 800-14: Category A--ADP resources in combat weapon systems and specially designed equipment; Category B--ADP resources in other systems developed under AFR 800-2; Category C--ADP resources in systems developed, acquired, and managed by AFR 80-2, AFR 65-2, AFR 71-11, and AFR 100-2; and Category D--ADP resources in general purpose, ADPS developed, acquired, and managed by the 300-series regulations and manuals. Primary application of risk assessment tools and methodologies will be to mission-critical ADP systems covered by categories A and B in accordance with AFR 800-14.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
I INTRODUCTION	I-1
1.1 BACKGROUND	I-1
1.2 STUDY OBJECTIVE	I-2
1.3 STUDY APPROACH	I-4
1.4 REPORT ORGANIZATION	I-5
II EXECUTIVE SUMMARY	II-1
2.1 INTRODUCTION	II-1
2.2 ANALYSIS CONDUCTED	II-1
2.3 PROPOSED RAMSS	II-2
2.4 RAMSS EVALUATION PROCESS	II-3
2.5 DEVELOPMENT AND IMPLEMENTATION FEASIBILITY	II-4
2.6 CONCLUSIONS OF STUDY	II-6
III IDENTIFICATION OF CANDIDATE RAMSS RISK MEASURES	III-1
3.1 BACKGROUND	III-1
3.1.1 Criteria and Constraints	III-1
3.1.2 Architectural Principles	III-1
3.1.3 Integration of Risk Concepts	III-3
3.1.4 Cross-sectional Nature of RAMSS	III-4
3.1.5 Dynamic Nature of RAMSS	III-5
3.2 RAMSS RISK MEASURES	III-5
3.2.1 Baseline SS Profile	III-5
3.2.2 SS Evaluation	III-8
3.2.3 Converting SS Evaluation Metrics to Risk Levels	III-18
3.2.4 SS Negative Outcomes	III-22
3.2.5 SS Magnitude of Consequence	III-23
IV USING AN RAMSS IN AN EVALUATION PROCESS	IV-1
4.1 INTRODUCTION	IV-1
4.2 LIFE CYCLE PHASES	IV-1
4.3 EVALUATION PROCESS OVERVIEW	IV-5
4.3.1 Planning for the Evaluation	IV-4
4.3.2 Conducting the Evaluation	IV-6
4.3.3 Analyzing the Evaluation Results	IV-6
4.3.4 Reporting the Results of an Evaluation	IV-8

TABLE OF CONTENTS (Concluded)

<u>Section</u>		<u>Page</u>
V	FEASIBILITY OF DEVELOPING AND IMPLEMENTING PROPOSED RAMSS AND ASSOCIATED MEASURES OF RISK	V-1
	5.1 INTRODUCTION	V-1
	5.2 FEASIBILITY ANALYSIS	V-1
	5.2.1 Establishing a Baseline SS Profile	V-1
	5.2.2 Development of Software Support Management Evaluation Metrics	V-2
	5.2.3 Upgrade of Current Software Supportability Evaluation	V-3
	5.2.4 Use of Operational Effectiveness Measures	V-3
	5.2.5 Interrelationships Among Evaluation Metrics	V-4
	5.3 DEVELOPMENT LEVEL OF EFFORT	V-5
VI	REFERENCES	VI-1
	APPENDICES	
A	ACRONYMS	A-1
B	GLOSSARY OF TERMS	B-1

LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
3-1	Software Supportability Risk Measure Derivation	III-6
3-2	Baseline ECS SS Maintenance Profile	III-9
3-3	Proposed Structure of Software Support Management Evaluation	III-11
3-4	Elements of AFOTEC Software Supportability Evaluation	III-14
3-5	Example Risk Probability Density Function (Maintenance Completion Time)	III-19
3-6	Example Risk Probability Density Function (Number of Maintenance Requests)	III-21
4-1	SS Risk Management Model Framework	IV-2
4-2	Integration of RAMSS and the Software Supportability Evaluation Process	IV-5

LIST OF TABLES

<u>Table</u>		<u>Page</u>
2-1	RA Data Base Summary	II-2
3-1	Proposed RAMSS Capability to Satisfy Criteria and Constraints	III-2
3-2	User/Supporter Baseline Profile Chart	III-10
3-3	Proposed Conversion of Metrics to Risk Levels	III-20
4-1	Expected Life Cycle Benefits of RAMSS	IV-3
4-2	Reporting RAMSS Results	IV-10
5-1	Development Requirements for the RAMSS Methodology	V-6

Section I

Introduction

SECTION I INTRODUCTION

1.1 BACKGROUND.

The Air Force Operational Test and Evaluation Center (AFOTEC) has the responsibility for conducting operational test and evaluation (OT&E) of assets entering the Air Force inventory. AFOTEC has developed and implemented various software OT&E methodologies. These methods have matured and have become the Air Force standard for evaluating software supportability. Each of these developed methods evaluates specific characteristics of the supportability aspects of delivered software and software support resources. These stand-alone evaluations provide AFOTEC with information to identify particular software supportability deficiencies, but do not identify overall risk associated with contractor or military ownership and organic maintenance of contractor-delivered software.

Assessing the software supportability risk of Air Force acquired systems is necessary to enable various decision makers to properly plan for system deployment. Risk assessment (RA) is required throughout the system acquisition life cycle. The perspective of OT&E is focused upon the overall system mission operation, including support. Methods are needed to provide software testers with areas which require testing emphasis, and decision makers with an assessment of the software supportability risk.

Software support for major weapon systems is becoming a major system cost factor. Major weapon systems are using more sophisticated computer systems and the support costs required for embedded software is projected to increase. Furthermore, since most enhancements to the system are dependent on software modifications, the timeliness of such software support is critical to system operational availability and effectiveness. Because of this criticality of the software support function to overall system mission operational capability, it is desired that top decision

makers be aware of the risk associated with the software supportability of a system at the conclusion of OT&E. In order to determine this risk during OT&E, AFOTEC needs to develop and implement a risk assessment model of software supportability with the proper system mission perspective to ultimately assist the top level decision maker. Due to the complexity of this requirement, it is first necessary to determine the feasibility of developing and implementing such a model.

AFOTEC produced a concept proposal (reference 6.12) for computer resources risk assessment during operational test and evaluation. This effort integrates an approach, appropriate models, and subjective and quantitative software operational and supportability measures into a management-oriented assessment of user and supporter risk. This initial involvement with the application of risk assessment to software supportability provided AFOTEC with justification to support a study of the feasibility of developing and implementing a risk assessment model for software supportability (RAMSS). The AFOTEC Subtask 304 (reference 6.0) is the statement of this feasibility study's objectives and required reports. This report documents the final part of this study.

1.2 STUDY OBJECTIVE.

The overall objective of this task study, as stated in Subtask Statement 304/00 (reference 6.0), is to perform a feasibility study to determine the level of effort and usefulness of developing and implementing a risk assessment model for software supportability (RAMSS). The first report of the subtask (reference 6.31) documents the first part of the effort: to "review defense and technical literature and current research concerning methods of software supportability testing and risk assessment applicable to an OT&E environment" (reference 6.0).

The emphasis for the first part of the task was placed upon:

- a) Identifying and collecting information
 - 1) Literature search and review
 - 2) Fact-finding visits/conference
 - 3) Contact with risk assessment/software experts.

- b) Assembling risk assessment data base
 - 1) Glossary of terms
 - 2) Annotated bibliography
 - 3) Key documents
 - 4) Experts/knowledgeable contacts list
 - 5) Current research list.

The second report of the subtask (reference 6.42) documents the second part of the overall task study: "based on the literature and research review, analyze the feasibility of developing and implementing a RAMSS that could be applied to the military systems during AFOTEC-conducted OT&E" (reference 6.0). The emphasis for the second part of the task was placed upon:

- a) Analyzing current literature and research
 - 1) DTIC, NTIS, NBS, RADC, AFOTEC, DoD, periodicals, etc.
 - 2) Potential RAMSS, or parts of RAMSS
 - 3) Continued contact with risk assessment/software experts.
- b) Developing a potential framework for a feasible RAMSS
 - 1) RAMSS framework
 - 2) Risk assessment methodologies, techniques, tools.

This report documents the third and final part of the overall task study: "identify candidate measures of supportability risk for use in developing a feasible RAMSS. Provide an analysis of how each measure would support a RAMSS that could provide usable and meaningful results to an overall assessment of software supportability risk" (reference 6.0). The emphasis for this part of the task was placed upon:

- a) Analyzing the candidate risk measures identified in parts one and two of this study
- b) Selecting the appropriate risk assessment methodologies which best permitted presentation of meaningful results
- c) Developing a model framework which integrated the theory of risk assessment with the software evaluation methodologies currently used by AFOTEC

- d) Analyzing the feasibility of developing and implementing the proposed risk assessment model.

1.3 STUDY APPROACH.

A three-step study approach was adopted in Subtask Statement 304/00. The steps were:

- a) Conduct a literature search and research review
- b) Analyze the literature and research information to determine the feasibility of developing and implementing a RAMSS to be applied to military systems during AFOTEC-conducted OT&E
- c) Identify and analyze candidate measures of supportability risk for use in developing a feasible RAMSS.

The first step results are presented in the report titled: "Software Supportability Risk Assessment in OT&E: Literature Review, Current Research Review, and Data Base Assemblage" (reference 6.31). The literature search and review required identification of key documents published by governmental agencies and civilian agencies. Literature searches of the Defense Technical Information Center (DTIC), National Technical Information Service (NTIS), and Rome Air Development Center (RADC) data bases were conducted. A search and review of National Bureau of Standards (NBS) publications was done. Key documents from these searches were identified and ordered for inclusion in the RA data base. Several documents from another AFOTEC subtask on Computer System Security (reference 6.32) were identified. The final report bibliography includes documents selected from that list. Researching the available RA technology also involved contact with a number of agencies, and identification of and discussions with RA research and evaluation personnel. The basic form and content of this data base of RA information is described in reference 6.31. The data base was augmented and updated as necessary to keep the data base current throughout this study.

The second step results are presented in the report titled: "Software Supportability Risk Assessment in OT&E: An Evaluation of Risk Methodologies" (reference 6.42). Analysis of candidate RAMSS involved analysis of literature and research collected from step 1 in the two areas of risk assessment and software supportability. Very little crossover between the two areas was evident. Hence, it was important for the feasibility requirement of this step to analyze the elements of risk assessment, factors of software supportability, and develop a framework within which it could be determined whether these "pieces" of a RAMSS could be integrated and implemented as a RAMSS.

The third step results are presented in this report. The analysis in the areas of risk assessment and software supportability performed in step two of this task formed the basis for the creation of the RAMSS model framework discussed in this report. This framework incorporates the software supportability evaluation tools currently being used by AFOTEC, and recommends additional measurement data be collected in the area of software support management. The collection and representation of measurement data are tied to the theoretical aspects of risk assessment.

1.4 REPORT ORGANIZATION.

This report is organized into six sections plus a set of appendices (acronyms and glossary). Report sections satisfy the following objectives:

- a) Section II contains an executive summary of the analysis conducted, candidate RAMSSs, the RAMSS evaluation process, development and implementation feasibility for the RAMSS, and conclusions from this study
- b) Section III contains a technical discussion of the RAMSS risk measures. A brief background presents the correlation of the theory of risk assessment with the process of evaluating software supportability. The RAMSS risk

measures are then discussed in more detail, particularly as those measures apply to the methods used for assessing risk

- c) Section IV contains a brief introduction to the software life cycle phases and discusses the assimilation of a risk assessment process, including reporting, with those phases
- d) Section V describes the feasibility of developing and implementing the proposed RAMSS and associated risk measures
- e) Section VI lists the documents whose contents have formed the basis for this report
- f) Appendix A lists acronyms used in this report
- g) Appendix B is a glossary of terms (sources of the terms and descriptions are listed) used in this report.

Section II

Executive Summary

SECTION II

EXECUTIVE SUMMARY

2.1 INTRODUCTION.

This section of the report provides an overview of the material presented in sections III through V. This overview summarizes the analysis conducted, describes the proposed risk assessment model for software supportability framework, identifies the selected measures of software supportability risk, and discusses the development and implementation feasibility.

2.2 ANALYSIS CONDUCTED.

The material analyzed during this study included documents obtained from the Defense Technical Information Center (DTIC); the Rome Air Development Center (RADC); the National Technical Information Service (NTIS); Risk Analysis (RA) experts and knowledgeable personnel contacted by telephone, on fact-finding trips and at conferences; and, references in key documents. The first report (reference 6.31) of this subtask contains the list of documents and sources which were used as a data base for this study. The major sources of documents, and the document counts, are given in table 2-1. The Computer System Security (CSS) task listed below includes data from reference 6.33.

Whereas a large number of documents were identified via the literature search on key words, it was found that a relatively small number of documents actually applied to the subject matter at hand. BDM personnel have obtained one-half of the total documents from other (experts, references in key documents, etc.) or in-house sources. Of the total of 148 documents, approximately one-fourth of them have been identified as "key" documents, in the sense that these documents contained information which was directly pertinent to the study of risk assessment of software supportability in the OT&E environment. These documents are listed

separately in section VI of this report, and form the basis for much of the analysis performed. Part of the count difference between documents ordered and received results from giving a count of one to received documents with more than one volume.

Table 2-1.
RA Data Base Summary

<u>Source of Data</u>	<u>Quantity of Documents Identified</u>	<u>Quantity of Documents Ordered</u>	<u>Quantity of Documents Received</u>
DTIC (1970-1984)	450	5	3
NTIS (1964-1984)	3000	53	38
RADC	3200	21	9
CSS TASK	16	16	15
AFOTEC	13	13	7
OTHER/IN HOUSE	76	76	76
	<u>6755</u>	<u>184</u>	<u>148</u>

2.3 PROPOSED RAMSS.

The conceptual risk assessment model for software supportability (RAMSS) incorporates a theoretical foundation for risk assessment with software evaluation tools presently being used by AFOTEC. The risk assessment methodologies chosen represent the authors' opinions of the most practical way to assess risk under the criteria and constraints with which AFOTEC must work and the software evaluation process in general. The AFOTEC software evaluation tools currently being used are described in AFOTECP 800-2, Volumes 1 through 5. Only a minor modification to these software tools (mostly administrative) would be required to integrate them with the proposed RAMSS.

The risk assessment methodology recommended involves the creation of probability density functions (PDFs) which represent the probability that a given outcome will occur. Important in this concept is the establishment of a baseline for the PDF by which positive and negative outcomes can be determined relative to that baseline. By proper representation of

the PDFs and their associated baseline, an analyst should be able to report the risk magnitude of a given outcome. Information on the severity of the outcome will also be present.

The establishment of baselines is obtained by historical data on similar systems and is further refined by user and supporter agreement on the maintenance action requirements for supportability. These actions may be identified using the following scheme:

<u>Maintenance Activities</u>	<u>Priority Types</u>	<u>Complexity Levels</u>
1. Correction	1. Normal	1. Low
2. Enhancement	2. Urgent	2. Medium
3. Conversion	3. Emergency	3. High

The combinations of the above actions yield various possible maintenance categories, for which baseline "values" must be defined. Data are collected for 1) required time to complete a maintenance request and 2) the number of expected changes in a given maintenance category per unit time.

Following the baseline establishment, the evaluation of risk is determined by using closed form questionnaires (current and new AFOTEC tools) to obtain the data necessary to produce the probability density functions. The evaluation is structured so the analyst can determine detailed information about which elements of supportability are driving the risk.

2.4 RAMSS EVALUATION PROCESS.

To be capable of maximum effectiveness, the RAMSS must be used throughout the software system's life cycle. Such application will achieve the following benefits:

- a) Early planning and trade-off studies for software support facility resource requirements.

- b) Early visibility of user requirements for expected software support actions.
- c) Early view of potential software support management problems.
- d) Capability to trace software supportability risk measures throughout the life cycle.

Proper application of the RAMSS evaluation is also required. This application involves:

- a) Planning evaluation
 - 1) Establish baselines
 - 2) Tailor baselines
 - 3) Establish evaluation structure for tools
- b) Conducting evaluation
 - 1) Calibrate evaluation questionnaire and evaluators
 - 2) Complete evaluation
- c) Analyzing evaluation results
 - 1) Compute measures of risk
 - 2) Construct risk probability density functions
 - 3) Compute support/user level of risk and risk drivers
 - 4) Perform trade-off analyses
 - 5) Determine evaluation reliability
- d) Reporting results
 - 1) To appropriate report level
 - 2) Highlight risk drivers
 - 3) Indicate alternatives
 - 4) Present consequences

2.5 DEVELOPMENT AND IMPLEMENTATION FEASIBILITY.

Throughout this study, there was an effort to identify an available RAMSS. No adequate models exist, hence an RAMSS has been proposed in this report. The feasibility of developing this RAMSS is reasonable, however there are some technical issues which need to be resolved before a full-scale development effort begins. These issues are described in

more detail in section V of this report. None of these issues is considered unresolvable. In summary, they may be grouped as follows:

- a) Establishing a baseline software supportability profile. The establishment of a baseline profile is dependent upon obtaining historical data and involving the user and supporter inputs. Depending upon the system, the baseline may be dynamic (changeable) up to the final OT&E evaluation. Cooperation among user, supporter, and evaluator (e.g., AFOTEC) to establish this baseline could be a problem for the AFOTEC.
- b) Development of Software Support Management evaluation metrics. The Software Support Management tool (recommended by this report) is not currently implemented by AFOTEC, and would have to be developed. (The availability of this tool is not critical to the full-scale development of the RAMSS, but it should be developed and implemented at a later date).
- c) Upgrade of current software supportability evaluation. The current tools used by AFOTEC would require modification to convert the evaluation metrics to measures of risk.
- d) Use of operational effectiveness measures. Operational effectiveness measures such as operator interface, test completeness and software maturity can be developed for inclusion in a model similar to the RAMSS. The risk baseline would be different (i.e., it would be related to operational requirements rather than support requirements).
- e) Interaction among evaluation metrics. The proposed methodology does not consider interrelationships between the software evaluation factors in the various tools. While an independence does not totally exist, there are methods which should be investigated to resolve this problem.

The resources necessary to develop and implement the RAMSS methodology are listed below. These resource estimates are preliminary and require further refinemen..

<u>Task</u>	<u>Resource Requirements</u>
1. Survey support facilities for historical baseline software support profile data	3 persons, 2 months
2. Develop RAMSS methodology	4 persons, 6 months
3. Conduct pilot study	3 persons, 1 month
4. Refine methodology	3 persons, 2 months
5. Develop/acquire/integrate requirements for automated support tools	2 persons, 1 month

2.6 CONCLUSIONS OF STUDY.

- a) No directly applicable RAMSS exists.
- b) It is feasible to develop an RAMSS
- c) The proposed RAMSS uses the foundation of risk assessment coupled with minor modifications to the tools for software evaluation currently used by AFOTEC.
- d) A continuation of the development and implementation of the proposed RAMSS is recommended.

Section III
Identification of Candidate RAMSS
Risk Measures

SECTION III

IDENTIFICATION OF CANDIDATE RAMSS RISK MEASURES

3.1 BACKGROUND.

This section discusses background information that is essential to understanding the risk assessment model for software supportability (RAMSS) and associated measures of risk. Five major topics are reviewed in this section: 1) the model criteria and constraints; 2) the architectural principles of the model framework; 3) how risk theoretical concepts are integrated into the model; 4) the model's cross-sectional nature; and 5) the model's dynamic nature. The basis for the RAMSS framework and associated measures of risk are described in detail in the previous report on evaluation of risk methodologies (reference 6.42).

3.1.1 Criteria and Constraints.

The report (reference 6.42) mentioned above presented some criteria for an RAMSS model and associated AFOTEC constraints on the use of any such model. Since these criteria and constraints greatly affect the framework of the RAMSS and the associated measures of risk, they are reiterated here (see table 3-1). Included in the table is a subjective assessment of how well the proposed RAMSS framework and software supportability risk measures presented in section III satisfy the criteria and constraints.

3.1.2 Architectural Principles.

The RAMSS framework was developed with the principles of risk theory and the practices of the AFOTEC Software Supportability Evaluation in mind. Section III describes the logical connections between risk theory, AFOTEC software supportability practices, and the RAMSS model framework.

Table 3-1.

Proposed RAMSS Capability to Satisfy Criteria and Constraints

RAMSS CRITERIA	POOR	FAIR	GOOD	EXCELLENT
a) HAS A TECHNICAL DEPTH AND RESULT FORMAT APPROPRIATE TO ADEQUATELY ASSIST DECISION.			X	
b) INTEGRATES AT LEAST THE CURRENT AFOTEC EVALUATION METHODOLOGIES.				X
c) HAS ENOUGH ACCURACY AND REPEATABILITY TO WARRANT CONFIDENCE IN ITS RESULTS.			X	
d) IS BASED UPON A SOUND THEORETICAL SOFTWARE AND RISK ASSESSMENT FOUNDATION.			X	
e) ALLOWS FOR DETERMINATION OF WHAT ACCEPTABLE LEVEL OF RISK MEANS DEPENDING UPON THE IDENTITY OF THE RISK AGENT AND THE SOFTWARE SUPPORTABILITY REQUIREMENTS.		X		
f) IS SIMPLE TO USE.				X
AFOTEC EVALUATION CONSTRAINTS				
a) RESOURCE LIMITATIONS 1) PERSONNEL 2) TIME 3) DATA COLLECTION (AVAILABILITY AND ACCURACY)			X	X X
b) VARIABLE ENVIRONMENT 1) COMPUTER 2) SOFTWARE 3) DEVELOPMENT 4) TESTING/TEST COVERAGE SCENARIO			X X X X	
c) EVALUATION REPEATABILITY AND UNDERSTANDABILITY 1) EVALUATOR EXPERIENCE 2) EVALUATION RELIABILITY 3) DEPTH OF EVALUATION MOES			X X X	
d) INTERNAL CHARTER 1) RESTRICTS CERTAIN OVERLAP AREAS (R&D) 2) EARLY LIFE CYCLE INVOLVEMENT NOT WELL DEFINED				X X

7611-1

3.1.3 Integration of Risk Concepts.

Three major concepts are inherent in the theoretical description of risk (reference 6.42). First, risk involves outcomes. Second, the outcomes are associated with some probability of occurrence. Third, the notion of a baseline is used to determine if an outcome is an unwanted, negative consequence. That is, a baseline determines negative outcomes from positive outcomes.

First, let us examine baselines. Baselines in risk theory can be logically connected to the necessary requirements for supporting a given piece of software. Hence, if the requirements for supportability are not met, then a negative consequence will have occurred. For example, assume that all emergency changes to software are required to be completed within 24 hours. If an emergency change actually takes 48 hours, then this is a negative outcome. Thus, a baseline, or requirement, must be determined to judge whether a given aspect of supportability is negative and undesired. Baselines are a necessary condition for risk assessment.

There are several different "baselines" which are integrated into the meaning of risk. There is the risk baseline, i.e., the definition of that profile of required outcomes against which negative outcomes (and positive outcomes) can be determined. There is a software baseline against which relative quality metrics can be determined. There is the OT&E threshold baseline (e.g., measures of effectiveness) such that any outcomes (e.g., evaluation measures) below the threshold are negative. It is also possible to establish low risk and high risk OT&E baseline metrics (e.g., software maintainability score of 3.3 for high risk and 5.0 for low risk). In this manner the outcome "scale" can be divided into three regions: low risk, medium risk, and high risk. In the case of software supportability risk being developed in this report, all these "baselines" will in fact be integrated but only the first (the risk baseline) will be what is termed the baseline software supportability (SS) profile. This baseline is discussed in section 3.2.1.

Outcomes are what could or does actually happen given the characteristics of the software maintainability, the support facility or the support management. Outcomes can be actual or predicted. For the most part the outcomes discussed in this report refer to those software maintenance outcomes predicted to occur during the software support phase. Hereafter, mention of outcomes in this report will thus mean predicted outcomes, unless otherwise qualified. Predicted outcomes are a function of heuristic estimation, historical data, and predictor experience. Actual outcomes form the data base of software maintenance activity at any given support facility. With each predictor outcome, some probability of that outcome's occurrence is attached.

3.1.4 Cross-sectional Nature of RAMSS.

The RAMSS may be applied at any point in time during the software life cycle. The ability to create time-frozen "snapshots" of the risk allows the evaluator to examine the risk drivers by looking at the groups of measures independently (under the current methodology). In this sense, the evaluator is looking at a "cross-section" of the software supportability evaluation process. At each snapshot, baselines may be reestablished (perhaps over previous best-guesses) to provide a more accurate evaluation. The current AFOTEC Software Supportability Evaluation scheme is the basis for the RAMSS model from a cross-sectional viewpoint.

Software supportability can be characterized as a hierarchy of evaluation characteristics. Software supportability is first broken down into three main areas: the software support facility, software product maintainability, and software support management. Each of these three major areas has subcategories. For instance, the software support facility includes personnel, support systems, and facilities. (For a complete description of the AFOTEC Software Supportability structure, see references 6.1 and 6.42.)

The hierarchical structure of AFOTEC's supportability scheme provides the option of risk assessment being conducted at various levels

of detail and depth. For example, a relatively "quick" risk analysis may be required; in this instance, only the higher level concepts in the hierarchy are investigated. If a fine-grained, detailed risk analysis is required, then the evaluation can be focused at the lower level of the supportability hierarchy. The hierarchical nature also allows analysis to be conducted at lower levels, yet be reported using the more general concepts found at the higher levels in the hierarchy.

3.1.5 Dynamic Nature of RAMSS.

The RAMSS is dynamic in nature. The assessment of risk for software supportability is done across the software life cycle from concept exploration through production and deployment. A high-level risk assessment of software is required early in the life cycle, preferably during concept exploration. Further risk analysis is required for major changes in system requirements which affect software requirements, and whenever major decision points are reached in the life cycle. This risk assessment may be conducted by the using command, development agency, support command, or an independent agency (e.g., during IV&V). The application of RAMSS is based upon the data available and the desired level of risk assessment.

Further aspects of using the RAMSS during the life cycle process are discussed in section 4.2.

3.2 RAMSS RISK MEASURES.

The following sections examine how a risk measure is derived for software supportability. The conceptual framework for the derivation of RAMSS measures is depicted by figure 3-1. (See reference 6.42 for a complete discussion of the RAMSS framework.)

3.2.1 Baseline SS Profile.

A baseline must be established in order for an assessment of risk to be made. In the software supportability context, the baseline(s) can be

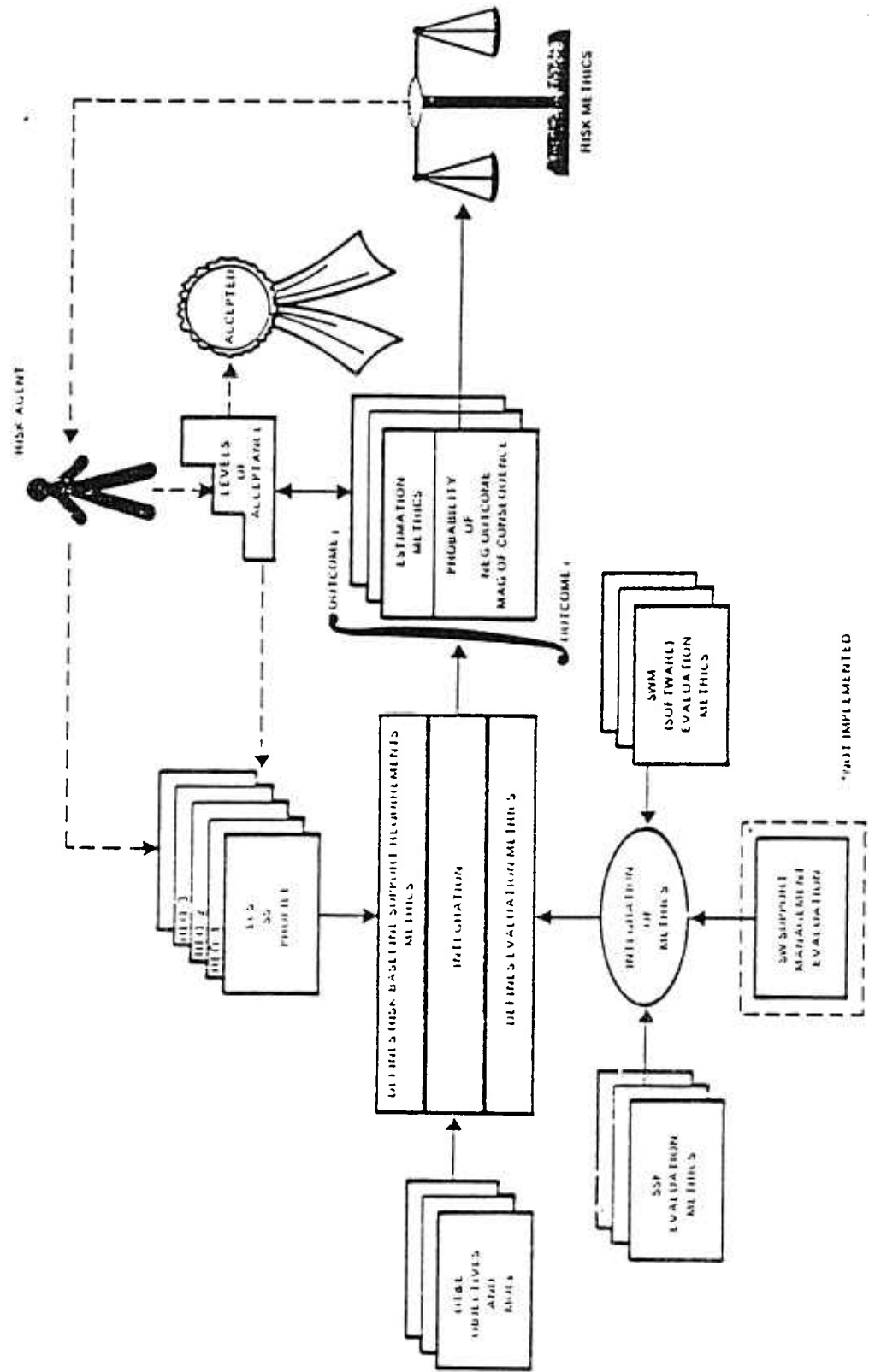


Figure 3-1. Software Supportability Risk Measure Derivation

equated with requirement(s) for supportability that have been established between user and supporter. (See section IV in this report for some aspects of defining these requirements).

Baseline values, or requirements, can be established for different types of software maintenance actions. The types are defined straight from the accepted definition of software maintenance. Recall that software maintenance activities are those for correction, enhancement, and conversion of the software. These three actions can have different priorities (depending on how critical completion is). The priority types conventionally used are: emergency, urgent, and normal. Further, associated with maintenance action and priority level is the complexity level involved in the maintenance. Conventionally, one of three complexity levels are specified: low, medium, and high. A full factorial combination of the maintenance action types, the priority types, and the complexity levels, yields 27 possible maintenance categories. Thus, 27 requirements, or baseline "values", must be defined; that is, one requirement exists for each maintenance action-priority-complexity type. A full profile of requirements is simply the consideration of each individual requirement all at once. In other words, a baseline profile is all 27 requirements for maintenance categories taken as a whole.

Several variables could be used to measure the baseline, or requirement, values. For instance, cost could be used: a normal correction of low complexity might have a cost requirement (or baseline) of 500 dollars. Any expense greater than 500 dollars for such a maintenance category action would be a negative outcome.

The variables chosen here to define the baseline value for each of the maintenance categories are:

TC - time (calendar) to complete the maintenance request (input to configured update).

NT - number of change requests in a given maintenance category per unit time (one year).

That is, the baseline maintenance profile can be represented as 27 pairs of numbers (TC, NT). These "time" variables were judged to be more directly related to maintenance activity than other choices, therefore

providing a more direct link between software supportability evaluation metrics and measures of software supportability risk.

As an example, suppose a 48-hour completion time requirement is placed upon urgent conversions of medium complexity. Also, it is required that 2 such urgent conversions of medium complexity be completed per month (each within 48 hours). Then the two-dimensional baseline value is the required time in which each individual maintenance type must be completed (48 hours), and the number of such maintenance types that must be completed per year (24). Figure 3-2 illustrates the three-dimensional nature of the baseline maintenance profile and the two-dimensional baseline value for each baseline maintenance category. Table 3-2 illustrates a chart form of the baseline maintenance profile data which could serve as the basis for a user and supporter agreement.

3.2.2 SS Evaluation.

The proposed software supportability (SS) evaluation follows the current thinking and practices of AFOTEC. That is, software supportability has three major subcategories: software support facility, software product maintainability, and (as proposed in this report) software support management (see figure 3-3). Each of these three areas is discussed in turn.

3.2.2.1 Software Product.

The expected outcomes and their probabilities of occurrence for the software product are a function ($\mathcal{F}$) of the evaluation measures, i.e.,

$$\begin{aligned} \text{maintenance outcome} &= (\text{time for maintenance, number of maintenance} \\ &\quad \text{requests}) \\ &= \mathcal{F} (\text{evaluation measures}) \end{aligned}$$

Note that the outcomes are defined using the same variables as used to establish the baseline. Thus, the outcomes are directly comparable to the baseline. The evaluation measures must be related to risk levels to complete the model. This conversion is illustrated in section 3.2.3.

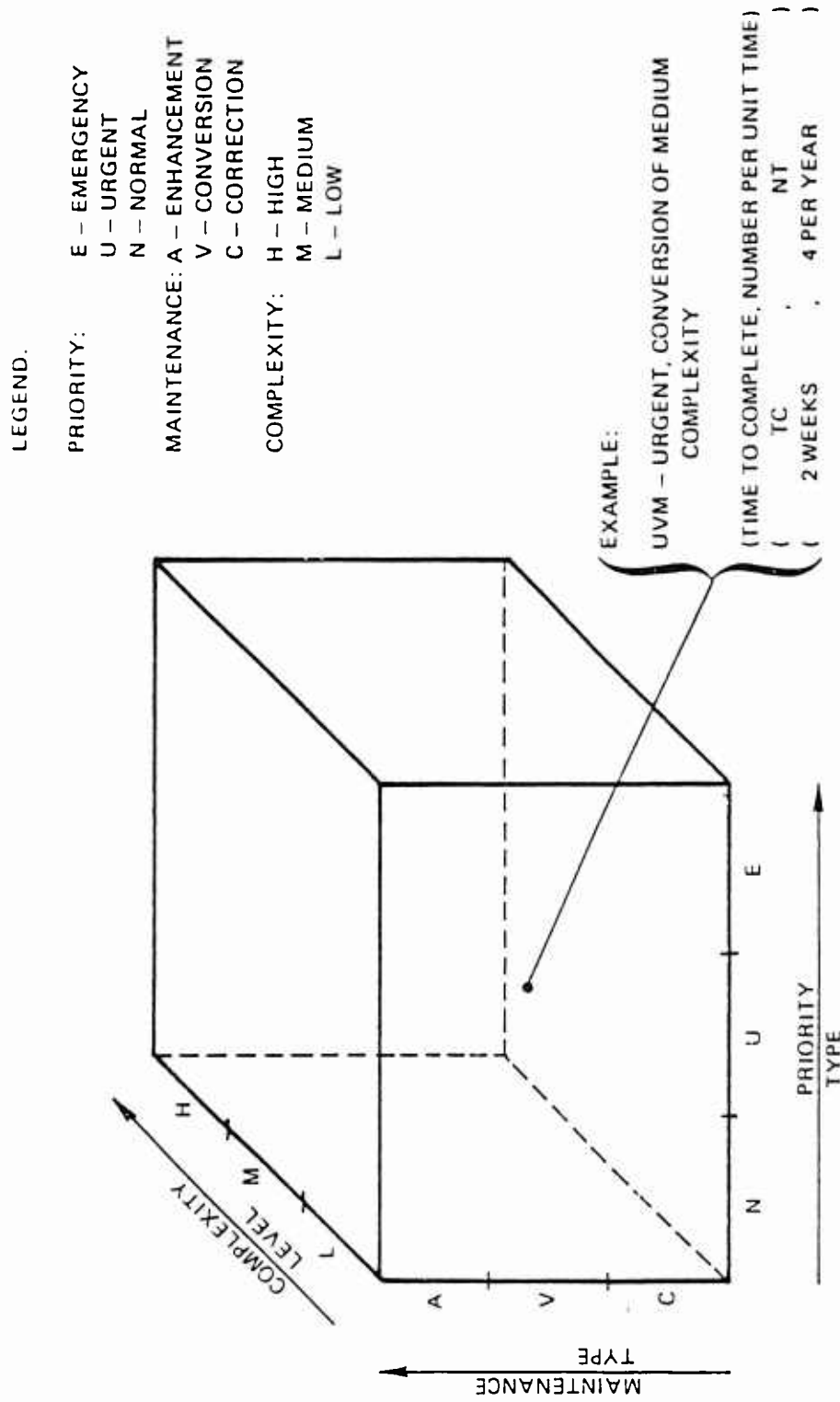


Figure 3-2. Baseline ECS SS Maintenance Profile

Table 3-2.
User/Supporter Baseline Profile Chart

PRIORITY TYPE	MAINTENANCE TYPE	COMPLEXITY LEVEL	TIME TO COMPLETE MAINTENANCE REQUEST	NUMBER OF MAINTENANCE REQUESTS PER UNIT TIME	COMMENTS
E	A	H			
		M			
		L			
	V	H			
		M			
		L			
	C	H			
		M			
		L			
U	A	H			
		M			
		L			
	V	H			
		M			
		L			
	C	H			
		M			
		L			
N	A	H			
		M			
		L			
	V	H			
		M			
		L			
	C	H			
		M			
		L			

LEGEND

PRIORITY TYPE
E EMERGENCY
U URGENT
N NORMAL

MAINTENANCE TYPE
A ENHANCEMENT
V CONVERSION
C CORRECTION

COMPLEXITY LEVEL
H HIGH
M MEDIUM
L LOW

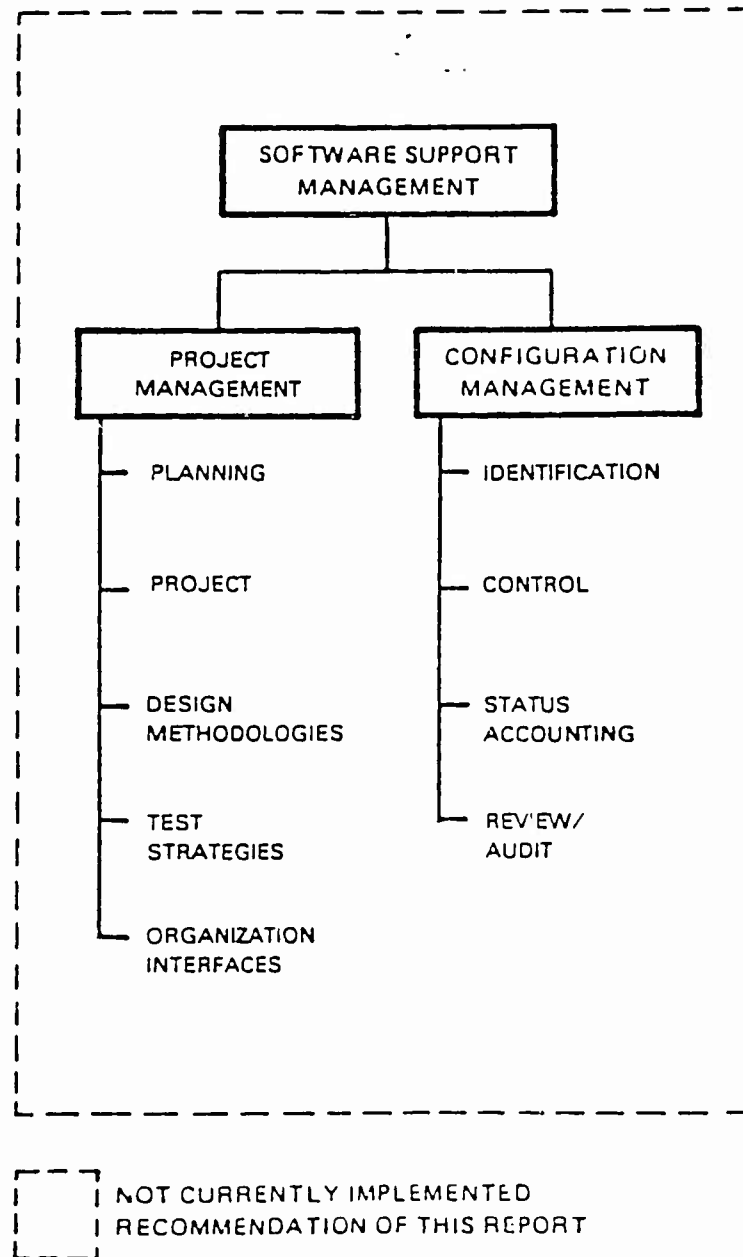


Figure 3-3. Proposed Structure of Software Support Management Evaluation

The evaluation measures come directly from the AFOTEC Software Supportability Evaluation scheme. As previously mentioned, this scheme is hierarchical in nature so the evaluation measures are thus hierarchically structured. Also, precise definitions exist for the evaluation measures. For example, at one level in the hierarchy

$$\begin{aligned}\text{maintenance outcome} &= (\text{time for maintenance, number of maintenance requests}) \\ &= f(\text{documentation, source})\end{aligned}$$

That is, documentation and source code evaluations determine the measures that determine the possible outcomes of maintenance time and maintenance requests along with each outcome's probability of occurrence.

At a lower, finer-grained level in the hierarchy,

$$\begin{aligned}\text{maintenance outcome} &= (\text{time for maintenance, number of maintenance requests}) \\ &= f(\text{documentation modularity, source code modularity, documentation descriptiveness, source code descriptiveness, documentation consistency, source code descriptiveness, documentation consistency, source code consistency, documentation simplicity, source code simplicity, documentation expandability, source code expandability, documentation instrumentation, source code instrumentation})\end{aligned}$$

At issue is whether the RAMSS should be conceptually considered a series of single regression formats, i.e.,

$$\begin{aligned}\text{maintenance outcome} &= f(\text{documentation}) \\ \text{maintenance outcome} &= f(\text{source code})\end{aligned}$$

or whether the RAMSS should be conceptually thought of as in a multiple regression format, i.e.

$$\text{maintenance outcome} = f(\text{documentation, source code}).$$

The obvious difference between these two formats is whether the risk measures are considered separately (as in the single regression format) or considered together (as in the multiple regression format).

The single regression format has a problem because the individual estimates of time for maintenance must be combined in some manner to come up with a composite estimate for product maintainability. On the other hand, the multiple regression format is a problem because the estimation process becomes more difficult due to the interaction effects of the different dependent variables (evaluation factors). The way in which the interaction effects are estimated may be different between individual evaluators. Thus, when some sort of questionnaire method is used, the multiple regression format is difficult to use. However, it is also a more realistic approach.

3.2.2.2 Software Support Facility.

The estimation of outcomes and their probabilities for the support facility follows the same format as is used for software product maintainability. Outcomes and their probabilities are a function of evaluation measures. The evaluation measures come directly from the AFOTEC Software Supportability Evaluation scheme, and are hierarchically structured allowing varying analysis and reporting.

At one level in the hierarchy,

maintenance outcome = (time for maintenance, number of maintenance requests)

= £ (personnel, support systems, facilities)

A further refinement in the level of detail of the evaluation measures can be found in figure 3-4.

3.2.2.3 Software Support Management.

The same logic is used in arriving at outcomes and probabilities for support management as was used for the other two major supportability

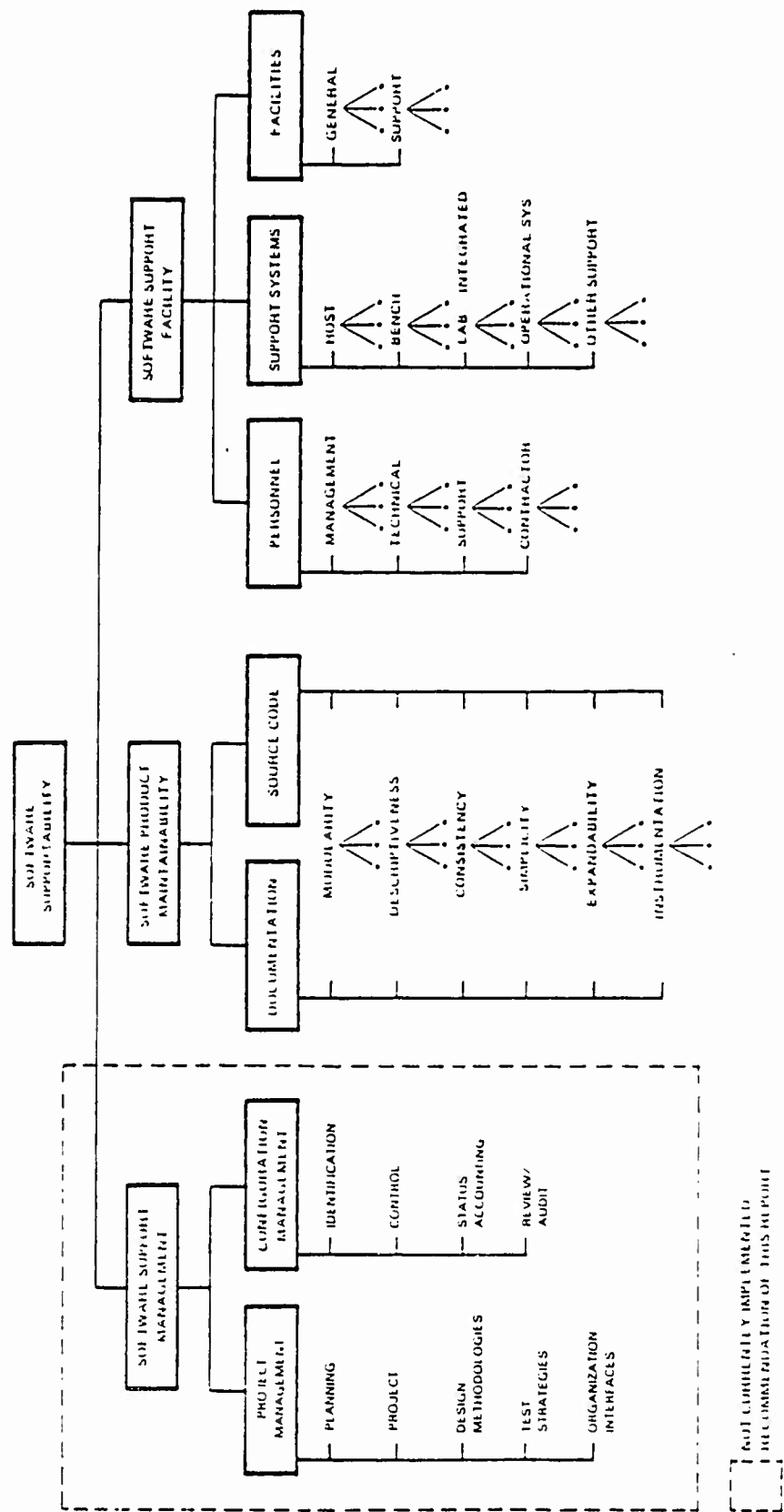


Figure 3-4. Elements of AFOIEC Software Supportability Evaluation

categories. Again, outcomes and probabilities are a function of evaluation measures. The evaluation measures come directly from the AFOTEC Supportability Evaluation scheme. At one level in the hierarchy, the outcomes and probabilities are a function of configuration management and project management, i.e.,

$$\begin{aligned}\text{maintenance outcome} &= (\text{time for maintenance, number of maintenance} \\ &\quad \text{requests}) \\ &= f(\text{configuration management, project} \\ &\quad \text{management})\end{aligned}$$

Configuration management is further broken down into: identification, control, status accounting, and review/audit. Project management is further broken down into: planning, project organization, design methodologies, test strategies, and organization interfaces (figure 3-4).

There is currently no implementation by AFOTEC of this part of the software supportability evaluation. More precise definitions and lower level factor characteristics would need to be developed. The RAMSS does not depend upon its use, nor does it rule out inclusion of other possible factors. Some aspect of developing and implementing this area of the software supportability evaluation is discussed in section 5.

3.2.2.4 SS Evaluation Metrics.

The vehicle for measurement of software supportability is a closed-form questionnaire. (See reference 6.42 for the full details of closed-form questionnaires.) The point of departure from previous AFOTEC questionnaires is the emphasis that the concept of the baseline is built into the questions themselves. In other words, the measurements of software supportability are made within the context of the established baseline requirements for supportability. In essence, the metrics are gauged with respect to a standard: the baseline value.

Each evaluation metric is a measure of a software supportability characteristic and is determined by evaluator response to a closed-form

questionnaire. The intent is to phrase the question with respect to the capability to satisfy the given baseline requirement. Thus, the evaluation metric is relative to the baseline value and when properly converted (see section 3.3) represents a risk measure relative to this baseline value.

More specifically, an example of an actual question might be:

- Q. Based on the software support facility, the given requirements can be met.

If a particular requirement is that low complexity emergency enhancements be completed in 48 hours, and 10 of these maintenance types must be completed per month, then the question becomes:

- Q. Based on the software support facility, low complexity emergency enhancements can be completed in 48 hours and 10 of these maintenance types can be completed per month.

Given that there are 27 possible maintenance categories (action, priority, complexity), then the entire baseline profile might be considered in the question, e.g.,

- Q. Based on the software support facility, the baseline (or requirements) profile can be met.

Because the evaluation measures are hierarchically structured, a finer set of metrics might be used to pinpoint where high risk might exist in the software support facility. The question above then becomes these three questions:

- Q. Based on the personnel, the baseline (or requirements) profile can be met.
- Q. Based on the support systems, the baseline (or requirements) profile can be met.
- Q. Based on the facilities, the baseline (or requirements) profile can be met.

A given software project may require a very fine-level analysis of the possible areas of high risk. The hierarchical nature of the evaluation measures allows for this more in-depth analysis. For example, the metric gauging personnel now becomes:

- Q. Based on the management, the baseline (or requirements) profile can be met.
- Q. Based on the technical personnel, the baseline (or requirements) profile can be met.
- Q. Based on the support personnel, the baseline (or requirements) profile can be met.
- Q. Based on the contractor, the baseline (or requirements) profile can be met.

These questions, or more accurately, requirements, are presented to one or more evaluators. Each evaluator responds to each question with an evaluation score from the scale below:

1	2	3	4	5	6
completely disagree	strongly disagree	generally disagree	generally agree	strongly agree	completely agree

The scale or evaluation scores are assumed to be consistent across the various questions. That is, a score of '6' means the same regardless of which question it is associated with. The scale is also considered to be metric in that the intervals between any two consecutive numbers are equal. This assumption of metric quality data may be problematic; however, the assumption is made as a starting point.

Ultimately, the metrics must be translated into some measure of risk. This transformation is discussed in section 3.2.3.

3.2.3 Converting SS Evaluation Metrics to Risk Levels.

The actual determination of risk comes from the metrics, or evaluation scores. First, in general terms, higher scores represent low risk situations in that the requirement(s) can be met. Low scores provided by the raters represent high risk situations. In this instance, the baseline most likely will not be met.

Because the evaluation scale is considered consistent across the entire set of evaluation questions, areas of high and low risk can be pinpointed. For example, the raters may give scores of '1' and '2' for the questions dealing with the software support facility. Further, scores of '5' and '6' may be given for the software product. In this example, it is obvious that the support facility is the high risk area for supportability.

The amount of risk can be defined quantitatively from the evaluation score(s). Specifically,

$$R = \text{Level of risk} = f(\text{evaluation metric}).$$

For a first approximation which behaves in a manner as described above we define:

$$R = 1 - \frac{M-1}{5}$$

where

R = risk or percentage of outcomes that are negative

M = evaluation metric or evaluation score.

For instance, assume that an overall average evaluation score is 4.0. Now, using the formula, or transformation, given above, risk is calculated as .40. (Note that when M = 3.0, then R = .60. The example using M = 4.0 produces R = .40 by coincidence.) That is, there is a

40 percent chance that the baseline cannot be met. If the requirement is for maintenance to be completed in 48 hours, then 40 percent of the maintenance requests will not meet the 48-hour deadline. Or, considering the number of requests per month, there is a 40 percent chance that the number of requests per month cannot be completed. Table 3-3 illustrates the conversion of evaluation metrics for the indicated range of metrics.

It is convenient to think of risk as a probability density function (PDF). First, consider the case: time for the completion of maintenance. Given an evaluation score of 4.0, we calculated that 40 percent of the outcomes would be negative, i.e., they exceeded the baseline. Figure 3-5 depicts the fact that 40 percent of the possible outcomes do not meet the requirement time of 48 hours. Conversely, 60 percent of the outcomes do not exceed the baseline.

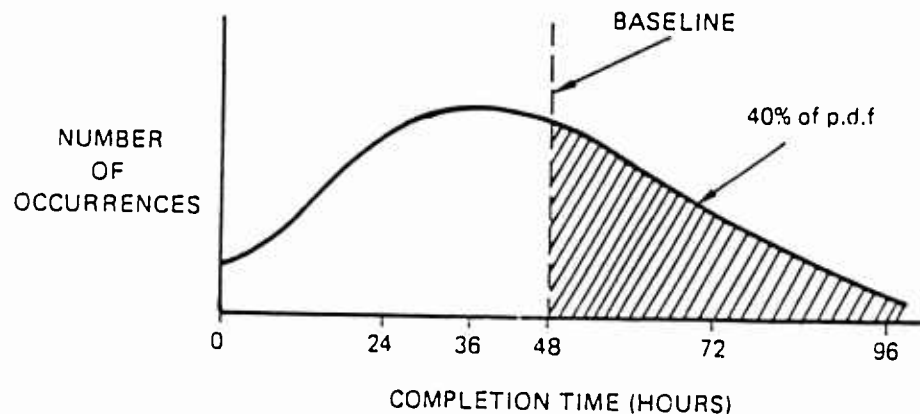


Figure 3-5. Example Risk Probability Density Function (Maintenance Completion Time)

Figure 3-5 gives us additional information about the time it takes to perform maintenance. More maintenance requests were made in "around 36" hours than for any other time. Relatively few maintenance requests required 96 hours to complete. Of all the negative outcomes, approxi-

Table 3-3.

Proposed Conversion of Metrics to Risk Levels

	SOFTWARE SUPPORTABILITY METRIC RANGE	RISK RANGE
6.0 LOW RISK	$5.0 \leq M \leq 6.0$	$0 \leq R \leq .2$
5.0 MEDIUM RISK	$3.3 \leq M < 5.0$	$.2 < R \leq .54$
3.3 HIGH RISK	$1.0 \leq M < 3.3$	$.54 < R \leq 1.0$
1.0	GENERAL CONVERSION FORMULA: $R = 1 - \frac{M - 1}{5}$ M = SOFTWARE EVALUATION METRIC R = RISK ASSOCIATED WITH METRIC	

mately 70 percent occurred between 48 and 72 hours. Thus, in this sense, the magnitudes of the negative outcomes are specified. Obviously, the magnitudes depend on the shape of the probability density function. The shape of the function is not given by a transformation of the metrics. Nevertheless, some general distribution form can be assumed or perhaps derived from historical support data. Perhaps a Poisson distribution is appropriate, because events occurring along a time continuum are often modelled using this functional form. All that would need be done is to relate the parameters of the Poisson model to an appropriate metric.

Figure 3-6 represents the same risk ideas, but for the number of requests per month. Remember that negative outcomes in this case are those outcomes which are less than the baseline value. We must be careful to distinguish between: 1) the case where the number of requests per month established as a requirement cannot be completed, and 2) the case where the number of requests per month did not exceed the requirement. In the first case, there is a negative outcome. In the second case, there is no negative outcome (from the user viewpoint at least). Notice that 40 percent of the PDF does not meet the specified requirement.

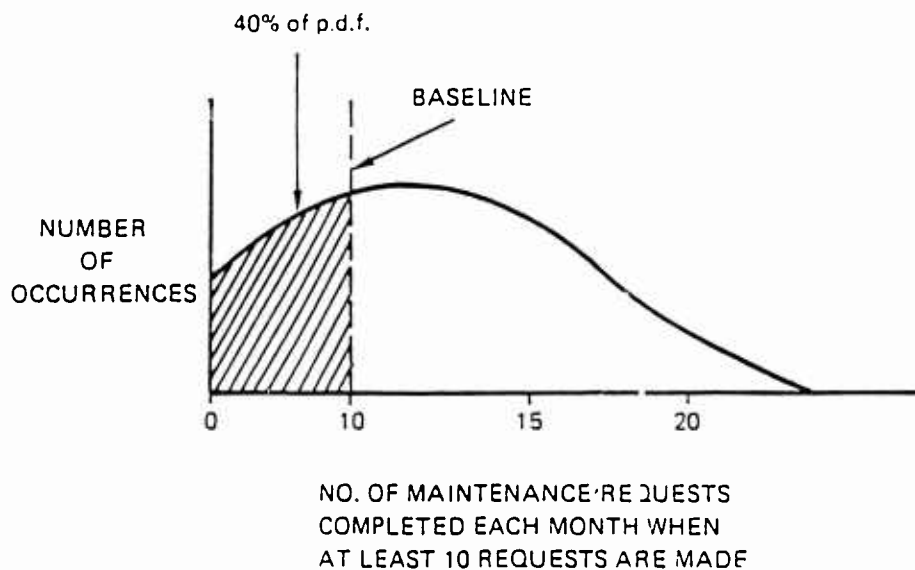


Figure 3-6. Example Risk Probability Density Function (Number of Maintenance Requests)

Another interesting user/supporter perspective can be derived from the probability density functions in figure 3-5 and 3-6. The purpose of the support function is to provide resources to satisfy the baseline maintenance profile. When resources are not sufficient or adequate to satisfy the baseline, then negative outcomes to the user (and supporter) are the result. However, if the baseline requirements are overestimated (i.e., the number of requests is actually less than the baseline requirement, or the stated maintenance completion time is less than actually necessary), then this can cause underutilization of support resources. This outcome can also be considered to be negative (at least to the support command). One value of the distribution function, as in figures 3-5 and 3-6, is that it provides a perspective on what the range of possible outcomes might be, so that peak and minimum support resources can be estimated and a plan for distributing such resources can be formulated. Determining what range is acceptable (to both user and supporter) is a function of the magnitude of the consequence of a negative outcome and the user/supporter willingness to accept the implied risk.

3.2.4 SS Negative Outcomes.

Quite simply, negative outcomes are those outcomes that do not meet the baseline requirement. For instance, let us assume that our requirement for low complexity, emergency enhancements is that: (1) they be completed in 48 hours, and (2) 10 such requests must be completed in a month. If a given low complexity emergency enhancement takes greater than 48 hours, then a negative outcome has occurred. Or, if 10 such maintenance types of this specification cannot be completed in a given month, then a negative outcome has occurred. As discussed in section 3.2.3, there are aspects of overestimating baseline requirements which can lead to negative outcomes because too many resources are being allocated. Further consideration of these aspects is beyond the scope of the current report, but should be considered during the full development of the RAMSS methodology (see section 5).

3.2.5 SS Magnitude of Consequence

The magnitude of each negative outcome to the user/supporter risk agent must also be considered. If a requirement is 48 hours for maintenance completion, then negative outcomes are any maintenance action requiring more than 48 hours. Thus, negative outcomes in this example can range from just longer than 48 hours to the point where the maintenance action was not even completed.

Some aspects of this magnitude were described as part of section 3.2.3. In general, the specific negative outcomes and their consequences must be considered relative to both user and supporter. We have presented a viewpoint based primarily upon the user requirements (as agreed to by the supporter). Thus, any negative outcome which reflects disparity from these requirements is both a user and supporter risk. The magnitude of the consequence of such risk to the user or supporter may well differ. In addition, some negative outcomes primarily from the supporter perspective have not been explicitly considered (see sections 3.2.3 and 3.2.4 for some details).

Section IV

Using RAMSS in an Evaluation Process

SECTION IV

USING AN RAMSS IN AN EVALUATION PROCESS

4.1 INTRODUCTION.

Section III describes elements of a proposed RAMSS framework and risk measures. To be effective, this model must be used as part of an overall software supportability evaluation process within a well-defined risk management structure. Figure 4-1 illustrates such a risk management structure. The RAMSS technical features of SS T&E and SS Risk Analysis are described in section III. This section will briefly consider some of the parts of the evaluation process to illustrate use of the proposed RAMSS. A more complete description of this process would be part of a RAMSS methodology development and implementation.

4.2 LIFE CYCLE PHASES.

Evaluation of software supportability is a life cycle process. There are key events throughout a software system's life cycle where application of the proposed RAMSS (or some part of the RAMSS) would be beneficial. Some of these expected benefits throughout a typical life cycle are summarized in table 4-1. Benefits which might occur include: early planning and trade-off studies for software support facility resource requirements; early view of potential software support management problems; early visibility of user requirements for expected software support actions; capability to trace software supportability risk profile (i.e., measures of risk) throughout the life cycle; early view of expected software supportability risk drivers; and, the actual assessment of the risk to user and supporter which must be accepted before support of the software can be assumed.

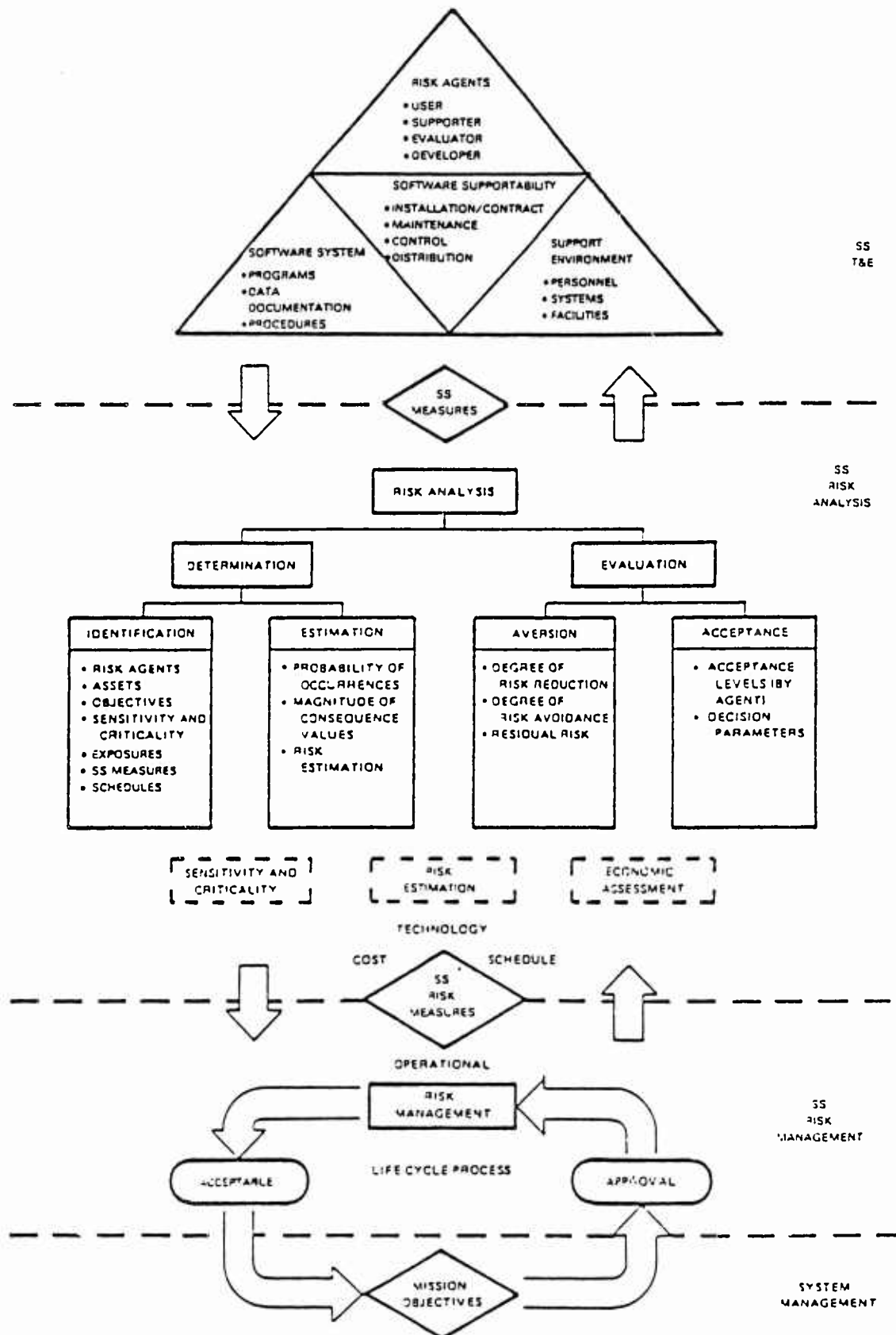


Figure 4-1. SS Risk Management Model Framework

ABZ-1. PEC-1. LIF. YCLL -NEF- - OF -SS

PHASE	USE OR ROLE OF RAMSS	EXPECTED BENEFITS
CONCEPT EXPLORATION (CONCEPT)	1. BASELINE SS PROFILE IS ESTABLISHED (FIRST CUT) BY AFOTEC WITH USER COMMAND AND SUPPORT COMMAND ASSISTANCE.	1. EARLY USER/SUPPORTER VIEW OF MAINTENANCE ACTIVITY. 2. INPUT TO SUPPORT REQUIREMENTS ASSESSMENT, TEMP, CRISP, AND O/S CMP FOR PLANNING PURPOSES. 3. BETTER ATTENTION TO SOFTWARE SUPPORT DURING EARLY SYSTEM REQUIREMENTS ANALYSIS. APPLY BASELINE PROFILE AGAINST HISTORICAL PROFILE FOR EARLY SUPPORT RESOURCE REQUIREMENTS PREDICTION.
DEMONSTRATION AND VALIDATION (DEFINITION)	1. PRELIMINARY RISK ASSESSMENT OF SOFTWARE SUPPORTABILITY AT VERY HIGH LEVEL BASED UPON DATA ACQUISITION REQUIREMENTS (DAH), STATEMENT OF NEED (SON), PROGRAM MANAGEMENT PLAN (PMP), DATA PROJECT PLAN (DPP), TEMP, CRISP, O/S CMP. 2. UPDATE OF BASELINE MAINTENANCE PROFILE.	1. EARLY RISK ASSESSMENT AGAINST WHICH TO TRACK VARIOUS MONITORING AND EVALUATING OF SS RISK ELEMENTS THROUGHOUT OTHER PHASES OF LIFE CYCLE. REFINEMENT OF BASELINE PROFILE. 2. DIRECT INPUT TO EXECUTIVE BRIEFINGS AND INTERIM QUICK-LOOK REPORTS.
FULL SCALE DEVELOPMENT (DEVELOPMENT AND TEST)	1. MONITOR DT&E/IV&V TO DETERMINE SOFTWARE RISK DRIVERS AND APPROPRIATE OT&E TEST STRATEGY TO STRESS DRIVERS. UPDATES PRELIMINARY RAMSS RESULTS AND BASELINE PROFILES. 2. COMPLETE FULL SCALE RISK ASSESSMENT OF SOFTWARE SUPPORTABILITY USING RAMSS. 3. SUPPLEMENTAL RISK ASSESSMENT OF OPERATIONAL EFFECTIVENESS (e.g., AFOTEC OPERATOR-MACHINE INTERFACE, SOFTWARE MATURITY, TEST COMPLETENESS EVALUATIONS) USING SIMILAR RAMSS TECHNIQUES. 4. USE RAMSS DISTRIBUTION FUNCTIONS FOR SENSITIVITY ANALYSIS AND TRADEOFF STUDIES AS TO ALTERNATIVE BASELINE MAINTENANCE ACTION USER AND SUPPORTER ACCEPTABLE LEVELS OF RISK.	1. UPDATED LOOK AT EXPECTED SOFTWARE SUPPORT REQUIREMENTS TO SATISFY BASELINE SS PROFILE. 2. ESTABLISH SOFTWARE SUPPORTABILITY RISK LEVEL FOR SUPPORT COMMAND. USED TO HELP PREDICT MAINTENANCE REQUEST DISTRIBUTION, AND ASSOCIATED MAINTENANCE SUPPORT REQUIREMENTS. ALSO USED TO ASSESS LIKELIHOOD THE SUPPORT RESOURCES ARE PROPERLY ALLOCATED TO MEET BASELINE MAINTENANCE PROFILE. IF THIS LIKELIHOOD IS POOR, THEN THE SUPPORT COMMAND MAY REQUEST IMPROVEMENT IN SOFTWARE SUPPORT FACTORS WITH HIGH RISK BEFORE ACCEPTING SUPPORT RESPONSIBILITY. 3. ESTABLISH SOFTWARE SUPPORTABILITY RISK LEVEL FOR USER COMMAND. USED BY SUPPORT AND USER COMMAND TO ASSESS LIKELIHOOD THAT BASELINE MAINTENANCE PROFILE CAN BE MET BASED ON THE CURRENT "OPERATIONAL" STATE OF THE SOFTWARE PRODUCTS. IF THIS LIKELIHOOD IS POOR, THEN THE SUPPORT COMMAND MAY NOT AGREE TO THE BASELINE. 4. REDUCE USER/SUPPORTER RISK; ESTABLISH LEVELS OF RISK FOR USER/SUPPORTER; PROVIDE PEAK LOAD ANALYSIS; DETERMINE OVER ALLOCATION OF RESOURCES. 5. DIRECT INPUT TO EXECUTIVE BRIEFINGS, INTERIM QUICK LOOK REPORTS, FINAL REPORT AND FINAL REPORT BRIEFINGS, LESSONS LEARNED REPORTS.
PRODUCTION AND DEPLOYMENT	1. ACTUAL SS PROFILE DATA IS COLLECTED ALONG WITH RESOURCE EXPENDITURES REQUIRED TO SATISFY THE ACTUAL PROFILE. RAMSS CAN BE USED AS APPROPRIATE FOR CONTINUED COMPARATIVE ANALYSIS AND PREDICTION OF SOFTWARE SUPPORTABILITY RISK LEVELS.	1. COMPARE WITH BASELINE MAINTENANCE PROFILE. EARLY COMPARISON OF ACTUAL VERSUS BASELINE VALUES CAN HELP IN THE DYNAMIC ALLOCATION OF SUPPORT RESOURCES FOR OPTIMUM EFFECTIVENESS, AND PREDICTION OF FUTURE RESOURCE REQUIREMENTS. 2. SINCE THE SS PROFILE IS A USER/SUPPORTER AGREEMENT, THE ACTUAL PROFILE CAN SERVE AS A LEVERAGE FOR EITHER USER OR SUPPORTER AT ANY TIME. DEPENDS UPON THE UNIFORM DISTRIBUTION OF THE MAINTENANCE ACTIVITY (ACROSS A DESIGNATED PERIOD OF TIME) IMPLIED BY THE BASELINE MAINTENANCE PROFILE AS COMPARED TO THE ACTUAL MAINTENANCE PROFILE AND ACTIVITY. 3. FEEDBACK THROUGH A GLOBAL DATA BASE OF ACTUAL SS PROFILE AND ACTIVITY SHOULD ALLOW FOR MORE ACCURATE ESTIMATES OF FUTURE BASELINE SS PROFILE DATA AND ASSOCIATED MAINTENANCE RESOURCE REQUIREMENTS. 4. ANALYSIS OF GLOBAL DATA BASE SHOULD ALLOW FOR REFINEMENT OF THE FUNCTION RELATING SOFTWARE SUPPORTABILITY EVALUATION METRICS TO RISK.

76115

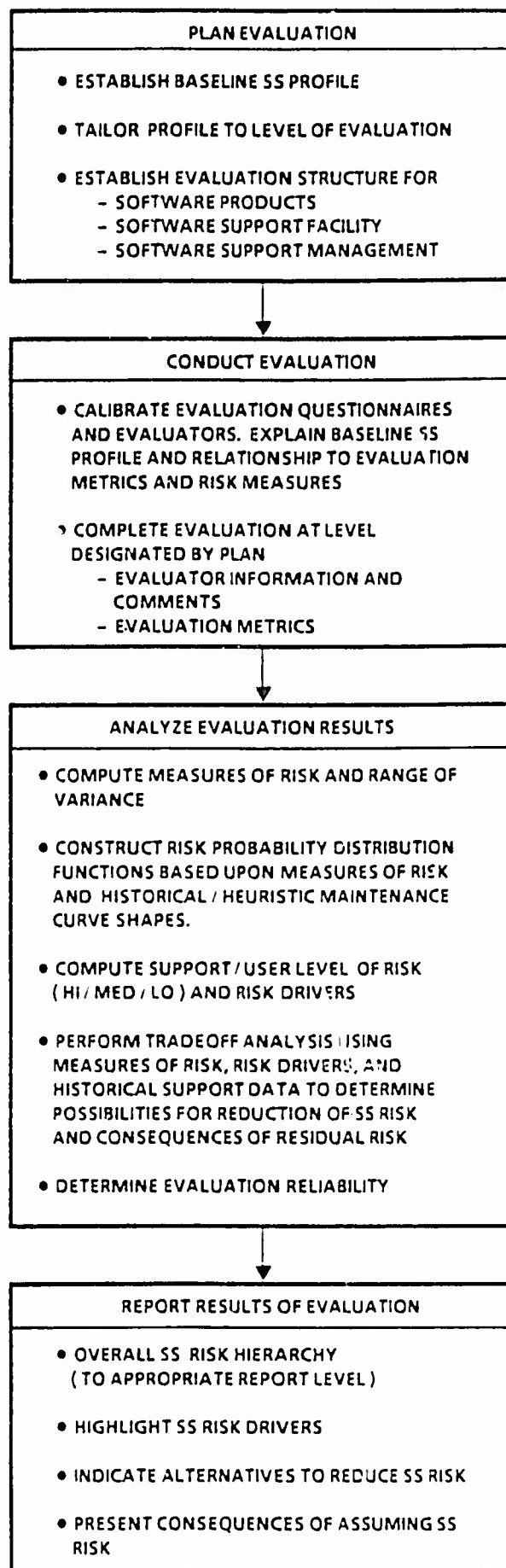
4.3 EVALUATION PROCESS OVERVIEW.

This section is not meant to replace development of a RAMSS methodology. It will serve to clarify the use of the RAMSS risk measures as described in section III, and as a point of departure for further methodology development. There are basically four parts to the evaluation process as illustrated in figure 4-2.

4.3.1 Planning for the Evaluation.

From the perspective of an RAMSS, the primary function in the planning phase is to establish an appropriate baseline SS profile. Because of the level of the evaluation being conducted, it may not be necessary to consider a full baseline profile. A more complete methodology should establish guidelines for collecting the baseline SS profile data and then tailoring the profile to requirements appropriate for the desired level of evaluation. Tailoring the data might involve "averaging" the data into a single baseline value with a specified range of variance. This would greatly simplify the evaluator effort, but might add uncertainty in the accuracy of the evaluation metrics.

The integration of the baseline SS profile as a reference point for each area of evaluation should be established by the more complete methodology. Since such a profile is likely to have a dynamic form tailored to each evaluation (perhaps even parts of the evaluation), it is likely that the evaluation questions should make some generic reference to the baseline SS profile as described in the evaluation guidelines. The level of evaluation (e.g., which factors and the depth of factor characteristics to be evaluated) will depend upon the phase of the software life cycle (see section 4.2) in which the evaluation is being conducted as well as the criticality of software to the mission function of the system. Each of the three major areas of evaluation must be structured so that desired evaluation metrics and associated measures of risk will be obtained in a form readily able to be incorporated into SS evaluation reports.



7611-2

Figure 4-2. Integration of RAMSS and the Software Supportability Evaluation Process

Other planning considerations such as weighting factors and other levels below these factors must be considered in light of their direct affect on risk assessment. This also can serve to distort the identification of actual risk drivers by the bias inherent in a subjectively determined weight. If factors and other level correlations are determined through regression analysis, then there is more basis for the combination. Still, as long as raw evaluation metrics are available, sensitivity analysis on these combinations (subjective weighting or regression) can be done.

4.3.2 Conducting the Evaluation.

Conducting the evaluation may occur over a short or long period of time depending upon the level of evaluating being conducted. All members of the evaluation team (test planners, test managers, evaluators, analysts) should be cognizant of the evaluation process and calibration requirements for the evaluation itself. It is this calibration which reduces the direct misunderstanding of what is to be evaluated, reduces the subjectiveness of the evaluation questions and responses, and improves evaluation accuracy and reliability.

The RAMSS has very little effect on complicating the already established AFOTEC evaluation itself, either technically or in consumption of evaluation resources (time and people). The evaluator does not need to understand risk or what is actually going to be done with the evaluation metrics to establish a level of SS risk. Thus the evaluation itself is essentially the same as is currently being used by AFOTEC and is described in reference 6.1.

4.3.3 Analyzing the Evaluation Results.

Most of the application of the RAMSS will be during the analysis of evaluation results. First, the evaluation metrics must be converted to risk measures as described in section 3.2.3. The conversion occurs at each level in the evaluation hierarchy after the evaluation metric for

that level has been computed using the typical AFOTEC weighted sum of components technique.

Since each evaluation question response (as the average of all evaluator responses) has a variance, there is an associated variance in the risk. This variance determines a measure of SS risk and an associated risk range for each level in the hierarchy.

The distribution of the risk around the baseline value can be estimated by using a hypothesized or actual historical SS profile probability density function (see section 3.2.3), the baseline SS profile requirements, and the computed measures of SS risk. This helps provide a perspective on the magnitude of the consequence of the computed SS risk. It also helps in the determination of the effects of peak and minimum SS resource loading.

From the computed measures of risk and the associated risk probability density function(s), the overall user risk and supporter risk is computed. A complete RAMSS methodology should provide guidelines on this computation.

The concepts presented in section III focus upon the "sufficiency" of resources, product quality, and so forth to meet established user/supporter baseline requirements. This establishes a common user and supporter risk. As mentioned briefly in section 3.2.3, there is also the added risk due to the "necessity" of resources, product quality and so forth to meet the established user/supporter baseline requirements. In this case, there are too many resources allocated, or the product quality is too high (that we should be blessed with such a problem), to support actual SS profile requirements because the baseline SS profile requirements were overestimated. This implies a poor utilization of resources has occurred with an associated economic impact.

The agent responsible for expending software support funds (probably the support command) would have additional risk due to these circumstances. A comparison of the baseline SS profile with historical data would help to identify the more obvious overestimations. Appropriate adjustment of the baseline requirements would then reduce the risk due to this situation. However, the predominant focus is on "sufficiency", and

unless the evaluation questionnaire structure is modified to consider both sufficiency and necessity, there will be some supporter risk not directly considered. Since the modification is perceived to be very complex, and the associated analysis of evaluation results even more complex, this approach has not been incorporated into the RAMSS.

From the computed measures of risk and the estimated risk probability density functions, it is possible to perform simple trade-off studies and sensitivity analysis. For example, one can identify directly the reduction in risk due to an improvement in an evaluation component. It may be possible to significantly reduce risk by appropriate upgrade of a few software support risk drivers. The possible tradeoffs to reduce SS risk is also easy to explain and is ideal for including in reports for top level decision makers.

By having a reasonably concise and simple representation of SS risk, the distribution of risk about the agreed-upon baseline SS profile, and alternative choices to reduce risk, it is a straightforward task to present this information to the user and supporter for acceptance. It may be that the level of risk of not being able to adequately support emergency requests in a unit time period is acceptable to the supporter, but not to the user. In this case, either the baseline SS profile must be changed (unlikely in this case), or the measures of risk must be reduced (i.e., the characteristics being evaluated must be improved). The alternative approaches to reducing SS risk can thus be easily identified, supported by evaluation data and the RAMSS, and implemented with reasonable assurance of an effective outcome. Furthermore, this process can be easily explained to the appropriate level of decision makers.

4.3.4 Reporting the Results of an Evaluation.

Perhaps the most important aspect of the RAMSS is the direct relationship of the evaluation metrics to the SS measures of risk and alternative choices to reduce SS risk which need to be reported. The consequences (in particular, magnitude of particular negative outcomes, and support resource commitments to reduce the number of negative outcomes)

of the measures of risk are not quite as directly understood or reportable. A more complete RAMSS methodology would provide guidance as to the estimation of these consequences.

The various levels of reporting and report constraints for AFOTEC is described in reference 6.40. The report types are discussed in relationship to the RAMSS in reference 6.42. The reporting of risk information derived from the integration of the RAMSS with a software supportability evaluation is illustrated in table 4-2.

TYPE REPORT RAMSS RESULTS	EXECUTIVE BRIEFINGS	INTERIM QUICK-LOOK REPORTS	FINAL REPORT	LESSONS LEARNED REPORTS	CONGRESSIONAL DATA SHEETS
1. TOP LEVEL SS RISK	●	●	●		●
2. COMPLETE SS RISK HIERARCHY		●	●		
3. SS RISK RANGE		●	●		
4. SS RISK DRIVERS	●	●	●	●	
5. SS RISK PDF			●		
6. USER / SUPPORTER LEVELS OF RISK	●	●	●		
7. TRADEOFF ANALYSIS ALTERNATIVE CHOICES TO REDUCE SS RISK	● (BOTTOM LINE)		●	●	
8. ESTIMATED CONSEQUENCES			●	●	
9. BASELINE SS PROFILE	● (BOTTOM LINE)	●	●	●	
10. ACTUAL SS PROFILE (HISTORICAL DATA)			●	●	

76113

Table 4-2. Reporting RAMSS Results

Section V

Feasibility of Developing and Implementing Proposed RAMSS and Associated Risk Measures

SECTION V

FEASIBILITY OF DEVELOPING AND IMPLEMENTING PROPOSED
RAMSS AND ASSOCIATED MEASURES OF RISK

5.1 INTRODUCTION.

The report on Evaluation of Risk Methodologies (reference 6.42) included a preliminary analysis of the feasibility of developing and implementing a RAMSS. This section extends that effort to include a more refined view of the proposed RAMSS and the associated measures of risk presented in this report. In addition, there are now some reasonable technical issues which need to be discussed as explanations of, and in some cases caveats to, the feasibility of accomplishing such a development. These technical issues are presented in section 5.2 as a summary of this feasibility analysis. The development and implementation of the proposed RAMSS with associated measures of risk is described in terms of the development tasks, and serves as a guideline for the level of effort required to accomplish the tasks.

5.2 FEASIBILITY ANALYSIS.

5.2.1 Establishing a Baseline SS Profile.

There will always be technical problems in establishing definitive requirements such as the Baseline SS Profile. The importance of obtaining this data is critical to the use of the proposed RAMSS.

It has been assumed that the best approach is for the user to "quickly" estimate the full profile during the software concept exploration life cycle phase. This estimate could be accomplished using historical profile data (if such data is available), a user's personal experience, and/or support command suggestions. Other sources of data for the users are possible. It may be necessary for the user and supporter to combine knowledge and produce an initial cut at the data.

It is also possible that a heuristic estimate by the evaluation agency (e.g., AFOTEC) may be necessary using the same sources as above,

but with the added burden of obtaining some level of agreement on the data values with both the user and supporter.

In any case, it should be stressed that the baseline SS profile is expected to be somewhat dynamic up to the final OT&E evaluation. Changes can be expected throughout the life cycle based upon new evaluation information and (perhaps) technological advances. It should therefore be clear that temporary acceptance of such a profile by the user and/or supporter does not commit the user and/or supporter to that profile forever. Hopefully, this baseline profile will evolve to be the "best guess estimate" of the actual SS profile data to be collected during the operation and maintenance phase. These caveats should make it easier to obtain user and supporter agreement so the further steps in the risk assessment process can be taken.

One aid to understanding this baseline profile would be an empirical data base gathered from actual support centers. This data collection task is suggested as part of the RAMSS methodology development.

Although there are some concerns about the technical (as well as logistical and political) feasibility of obtaining an accurate baseline SS profile, it is not resource bound. It is simply a matter of making reasonable estimates. It is expected that this will be feasible within the refinements which will result from the complete RAMSS methodology development.

5.2.2 Development of Software Support Management Evaluation Metrics

This area of evaluation is not currently implemented by AFOTEC. It is a recommendation of this report that a factor hierarchy similar to the other current AFOTEC software supportability evaluations be developed for software support management. It is not critical to the operation of the proposed RAMSS, but such an implementation should provide invaluable data concerning the software support management concerns across the life cycle process.

The feasibility of accomplishing the development of these evaluation metrics is very good. There are no known technical restrictions and the

emphasis in this area is justified by the recent software maintenance literature (see reference 6.31 and 6.42). It should be emphasized that factors and characteristics in this area would cover software management procedures, practices, standards, and so forth in both development and maintenance phases of the software. Frequently the management function in both phases (including the transition) is very important to the overall software supportability cohesion. The major factors of project management and configuration management (see section 3.2.2.3), besides capturing the essence of software support management, illustrate this requirement for cohesion. If implemented, there would be additional requirements for evaluation resources. With some care, this requirement should be within current AFOTEC constraints.

5.2.3 Upgrade of Current Software Supportability Evaluation.

Because of the necessity to evaluate relative to a baseline requirement (i.e., the baseline SS profile) in order to convert the evaluation metrics to measures of risk, the current evaluation questionnaires and evaluation procedures would have to accommodate this change. Since this change can be taken care of in an administrative fashion (e.g., guidelines to the evaluators), at least for the initial RAMSS methodology development, the impact upon the current mode of operation would be minimal. Integration of the refined methodology into the current evaluation process would be straightforward and might be combined with a more general upgrade of the evaluation questionnaires and procedures, or separately done.

5.2.4 Use of Operational Effectiveness Measures.

The operational effectiveness measures, such as the operator interface evaluation measures, test completeness measures, and software maturity measures, have not been discussed in any detail. It is possible to use these measures as part of the input to the proposed RAMSS. Similar considerations for other AFOTEC evaluations apply, but the proposed RAMSS must be applied indirectly.

It should be emphasized that these effectiveness measures do not indicate either user or supporter risk relative to the specified baseline SS profile. These metrics indicate something about the current operational status of the software. If the evaluation metrics are poor, then one might suspect there will be more software supportability risk relative to the baseline SS profile (which is presumably based upon software meeting specification requirements and having a good operational status). This in turn would cause the user to have more risk relative to the agreed upon baseline SS profile. Note, however, that the operational effectiveness evaluation metrics are not relative to the baseline SS profile, but are relative to some other baseline operational requirements.

The integration of operational effectiveness measures might be considered during the development of the RAMSS methodology. At this time this integration does not appear to be straightforward. The issue of having multiple baselines against which an evaluation is conducted can be confusing and derived metrics are not directly comparable.

5.2.5 Interrelationships Among Evaluation Metrics.

In section III there was some discussion about the assumption of independence of factors, with the caveat that interrelationships do, in fact, exist. The usual technique to determine interrelationships is to use parametric methods such as factor analysis and regression analysis.

The current AFOTEC technique is to simply take a weighted sum of components to determine the evaluation metric at each level. Due to the complexity of parametric analysis without known validated data, it is recommended that AFOTEC retain the weighted sum concept as part of the RAMSS methodology. However, during the proposed support facility data collection effort and pilot study to establish a historical baseline SS profile, it is recommended that parametric analysis be used to study possible interrelationships. It is not anticipated that such analysis will alter the RAMSS methodology development.

5.3 DEVELOPMENT LEVEL OF EFFORT.

The recommended tasks and associated level of effort to develop a RAMSS methodology are illustrated in table 5-1. The development tasks include: collection of data from current software support facilities to establish a historical baseline SS profile; completion of the theoretical foundation of the RAMSS; upgrade of the software supportability evaluation methodology to incorporate the RAMSS; a pilot study using a preliminary guidebook for assessing software supportability risk using the RAMSS; and refinement of the RAMSS methodology and guidebook based upon the pilot study "lessons learned."

The task to integrate requirements for automated support tools is primarily for risk assessment analysis and the supportability evaluation tools which already exist and are used, but which are not integrated into a cohesive system of tool support. These tools are used to provide the necessary statistical analysis, risk computation, and bookkeeping functions which will be part of the RAMSS methodology.

It should be emphasized that the projected level of effort (resource requirements) is a preliminary estimate at this time.

TASK	FUNCTIONAL DESCRIPTION	PRODUCTS	RESOURCE REQUIREMENTS
1. SURVEY SUPPORT FACILITIES FOR HISTORICAL BASELINE SS PROFILE DATA	SELECT SITES CONDUCT SURVEY PERFORM ANALYSIS OF DATA	SURVEY REPORT HISTORICAL BASELINE SS PROFILE	2 MONTHS 3 PERSONS
2. DEVELOP RAMSS METHODOLOGY	SPECIFY REQUIREMENTS/ASSUMPTIONS DESIGN RAMSS DEVELOP RAMSS PROCEDURES PRODUCE DRAFT RAMSS OT&E GUIDELINES HANDBOOK - DATA COLLECTION - EVALUATION PROCEDURES - RISK ASSESSMENT ANALYSIS - REPORTING TECHNIQUES	RAMSS METHODOLOGY REPORT (DRAFT) RAMSS OT&E GUIDELINES HANDBOOK (DRAFT)	6 MONTHS 4 PERSONS
3. CONDUCT PILOT STUDY	SELECT SOFTWARE PROJECT APPLY DRAFT RAMSS OT&E GUIDELINE HANDBOOK ANALYZE RESULTS	LESSONS LEARNED STUDY REPORT	1 MONTH 3 PERSONS
4. REFINE METHODOLOGY	REFINE REQUIREMENTS AND RAMSS METHODOLOGY REFINE RAMSS OT&E GUIDELINES HANDBOOK	RAMSS METHODOLOGY REPORT (FINAL) RAMSS OT&E GUIDELINES HANDBOOK (FINAL) EXECUTIVE BRIEFINGS ON RAMSS METHODOLOGY	2 MONTHS 3 PERSONS
5. DEVELOP/ACQUIRE/INTEGRATE REQUIREMENTS FOR AUTOMATED SUPPORT TOOLS	IDENTIFY ANALYSIS TOOLS TO SUPPORT RAMSS INTEGRATE TOOLS USED WITH RAMSS METHODOLOGY	VOLUME II OF RAMSS OT&E GUIDELINES HANDBOOK (AUTOMATED TOOL SUPPORT)	1 MONTH 2 PERSONS

7611-4

Table 5-1. Development Requirements for the RAMSS Methodology

Section VI

References

SECTION VI

REFERENCES

- 6.0 "Software Risk Assessment in OT&E," Final Subtask Statement 304 for AFOTEC Contract F29601-80-C-0035, AFOTEC, Kirtland AFB, NM, Apr 84.
- 6.1 AFOTEC 800-2 Volumes 1 through 5, Software OT&E Guidelines.
- 6.2 FIPS PUB 31, "Guidelines for ADP Physical Security and Risk Management," National Bureau of Standards, Jun 74.
- 6.3 FIPS PUB 65, "Guidelines for Automatic Data Processing Risk Analysis," National Bureau of Standards, Aug 79.
- 6.4 AFR 205-16, "Automatic Data Processing (ADP) Security Policy, Procedures, and Responsibilities," Attachment 5: Guidance for Performing Risk Analysis, 1 Aug 84.
- 6.5 OPNAVINST 5239.1A, "Department of the Navy Automatic Data Processing Security Program," Appendix E: Risk Assessment Methodology, 3 Aug 82.
- 6.6 Lathrop, F., "Alternative Methods for Risk Analysis: A Feasibility Study," Air Force Computer Security Program Office, 1 Sep 81.
- 6.7 Neugent, W., "Technology Assessment: Methods for Measuring the Level of Computer Security," Section 4.2: Risk Assessment Methodologies, National Bureau of Standards, Draft, Sep 81.
- 6.8 RADC, "Reliability Model Demonstration Study," RADC-TR-83-207, Volumes I and II, Aug 83.
- 6.9 Directorate of Aerospace Safety, "A Risk Management Guide for Air Force Operations," Air Force Inspection and Safety Center, Norton AFB, CA, 6 Nov 79.
- 6.10 USAF Scientific Advisory Board, "The High Cost and Risk of Mission-Critical Software," USAF SAB Ad Hoc Committee, Dec 83.
- 6.11 Fisher, G. and Lt. Col. E. Gay, "An Approach to Risk Analysis: A Process View," AF/SA Technical Note, Jun 81.
- 6.12 Fisk, F., and W. Murch, "A Proposal for Computer Resources Risk Assessment During Operational Test and Evaluation," AFOTEC Draft Report, 3 Oct 83.

- 6.13 Peercy, D., "A Framework for Software Maintenance Management Measures," Proceedings of the Seventeenth Annual Hawaii International Conference on System Sciences, Jan 84.
- 6.14 Peercy, D., and G. Swinson, "A Software Support Facility Evaluation Methodology," Proceedings of Symposium on Application and Assessment of Automated Tools for Software Development, Nov 83.
- 6.15 Booch, G., Software Engineering with Ada, Reading, MA: Benjamin/Cummings, 1983.
- 6.16 LeBlanc, R., and J. Goda, "Ada and Software Development Support: A New Concept in Language Design," Computer, 15(1982), 5, pp. 75-82.
- 6.17 Howden, W., "Contemporary Software Development Environments," Communications of the ACM, 25(1982), 5, pp. 318-329.
- 6.18 Lientz, B., and E. Swanson, Software Maintenance Management, Reading, MA: Addison-Wesley, 1980.
- 6.19 Lientz, B., and E. Swanson, "Problems in Application Software Maintenance," Communications of the ACM, 24(1981), 11, pp. 763-769.
- 6.20 GAO Report, "Federal Agencies Maintenance of Computer Programs: Expensive and Undermanaged," AFMD-81-25, Feb 81.
- 6.21 Parikh, G., Techniques of Program and System Maintenance, Cambridge, MA: Winthrop, 1982.
- 6.22 Thayer, R., A. Pyster, and R. Wood, "Validating Solutions to Major Problems in Software Engineering Project Management," Computer 15(1982), 8, pp. 65-77.
- 6.23 Boehm, B., J. Brown, and M. Lipow, "Quantitative Evaluation of Software Quality," Proceedings 2nd International Conference on Software Engineering, San Francisco, CA: 1976, pp. 592-605.
- 6.24 McCall, J., and M. Matsumoto, "Software Quality Measurement Manual," RADC-TR-80-109, Vol II (of two), Apr 80.
- 6.25 Rowe, W., An Anatomy of Risk, J. Wiley and Sons, New York, 1977.
- 6.26 Atzinger, E., and Brooks, W. (eds), "A Compendium on Risk Analysis Techniques," Aberdeen Proving Grounds, U.S. Army Materiel Systems Analysis Agency, 1972.
- 6.27 Megill, R., An Introduction to Risk Analysis, Petroleum Publishing, Tulsa, 1977.

- 6.28 Efron, B., The Jackknife, Bootstrap and Other Resampling Plans, Society for Industrial Mathematics, Philadelphia, 1982.
- 6.29 Worm, G., "Applied Risk Analysis with Dependence Among Cost Components," Clemson University Department of Industrial Management, 1981.
- 6.30 Rescher, N., Risk, Washington, D.C.: University Press of America, 1983.
- 6.31 Hoessel, W., W. Huebner, D. Peercy, G. Richardson, "Software Supportability Risk Assessment in OT&E: Literature Review, Current Research Review, and Data Base Assemblage," BDM/A-84-322-TR (Final), The BDM Corporation, September 1984.
- 6.32 "Analysis Support for Computer System Security OT&E," Final Subtask Statement 294 for AFOTEC Contract F29601-80-C-0035, AFOTEC, Kirtland AFB, NM, Jan. 1984.
- 6.33 Leibowitz, S., S. Parratto, D. Peercy, H. Pringle, J. Wiley, E. Witzke, "Computer System Security (CSS) Literature Review, Current Research Review, and Data Base Assemblage," BDM/A-84-108-TR (Interim), The BDM Corporation, May 1984.
- 6.34 Parratto, S., D. Peercy, H. Pringle, "Computer System Security (CSS) Test and Evaluation (T&E) Life-Cycle Process Definition," BDM/A-84-320-TR (Final), The BDM Corporation, August 1984.
- 6.35 Defense Systems Management College, Risk Assessment Techniques, Fort Belvoir, Virginia, July 1983.
- 6.36 Apostolakis, G., "Bayesian Methods in Risk Assessment," Advances in Nuclear Science and Technology, New York: Plenum, 1981.
- 6.37 Behm, R. D., J. W. Vaupel, Quick Analysis for Busy Decision Makers, New York: Basic Book, 1982.
- 6.38 Pritsker, A. A. B., C. D. Regden, Introduction to SLAM and Simulation, New York: John Wiley, 1979.
- 6.39 DeMillo, R., "A Risk Model for Software Testing," Georgia Tech University, Briefing Slides, July 20, 1984.
- 6.40 AFOTECR 55-1(C2), "OT&E Reporting," Chapter 6, March 15, 1984.
- 6.41 Peercy, D., "A Software Maintainability Evaluation Methodology," Transactions on Software Engineering, Vol. 7, No. 4, July 1981.
- 6.42 Huebner, W., D. Peercy, G. Richardson, "Software Supportability Risk Assessment in OT&E: An Evaluation of Risk Methodologies," (Final), BDM/A-84-496-TR, Aug 1984.

Appendix A

Acronyms

APPENDIX A
ACRONYMS

ADP	Automatic Data Processing
AFOTEC	Air Force Operational Test and Evaluation Center
CRISP	Computer Resources Integrated Support Plan
CSS	Computer System Security
DoD	Department of Defense
DTIC	Defense Technical Information Center
DT&E	Developmental Test and Evaluation
ECS	Embedded Computer System
IV&V	Independent Verification and Validation
NBS	National Bureau of Standards
NTIS	National Technical Information Service
OT&E	Operational Test and Evaluation
O/S CMP	Operational/Support Configuration Management Plan
PDF	Probability Density Function
RA	Risk Assessment
RADC	Rome Air Development Center
RAMSS	Risk Assessment Model for Software Supportability
SS	Software Supportability
TEMP	Test and Evaluation Master Plan
T&E	Test and Evaluation

Appendix B

Glossary of Terms

APPENDIX B
GLOSSARY OF TERMS

B.1 INTRODUCTION.

The glossary of terms for the Analysis of Software Supportability Risk Assessment Models varied as the project progressed. Refer to BDM/A-84-322-TR, (Final) dated September 28, 1984, for the complete glossary of terms.

Some terms have more than one description; when this is the case, the descriptions either:

- a) Are significantly different between sources (though the effective meaning may be not much different).
- b) Are used differently (different users or technical language).
- c) May be found within the context of a different source.
- d) Have real differences in meaning.

Both DoD and non-DoD (e.g., FIPS PUBs, NBS Special Publications) sources are used. The non-DoD sources and terms are not mandated for our use, but are rather included for breadth of understanding, for those relevant terms commonly used within the non-DoD governmental and/or private sectors.

The source of each description is indicated by a symbol in parentheses before that source's term description:

```
TERM1
  (SYMBOL1.1)
  Description1.1...
  (SYMBOL1.2)
  Description1.2...
  .
  .
  (SYMBOL1.n)
  Description1.n...
```

$TERM_2$.
.
. $TERM_N$

The symbols used and corresponding sources are:

- (AFOTEC1) AFOTEC 800-2, Volume 1, 10 Nov 82, "Software Test Manager's Guide."
- (AFOTEC3) AFOTEC 800-2, Volume III, 1 Jan 84, "Software Maintainability Evaluator's Guide."
- (AFR800-14) Air Force Regulation 800-14, Volume I, "Management of Computer Resources in Systems," 12 Sep 75.
- (AFR300-15) Air Force Regulation 300-15, "Automated Data System Project Management," Jan 78.
- (AFOTEC5) AFOTEC 800-2, Volume 5, 25 Jul 83, "Software Support Facility Evaluation--User's Guide."
- (ROWE) Rowe, William, An Anatomy of Risk, John Wiley, 1977.
- (LATHROP) Lathrop, Frank, "Alternative Methods for Risk Analysis: A Feasibility Study," Air Force Computer Security Program Office, 1 Sep 81.
- (AFR205X) Air Force Regulation 205-16, "Automatic Data Processing (ADP) Security Policy, Procedures and Responsibilities," 1 Aug 84.
- (CURRENT) Current document definition.

8.2 GLOSSARY OF TERMS FOR THE ANALYSIS FOR DETERMINING FEASIBILITY OF DEVELOPING AND IMPLEMENTING A RISK ASSESSMENT MODEL FOR SOFTWARE SUPPORTABILITY.

Accuracy

(ROWE)

The quality of being free from error. The degree of accuracy is a measure of the uncertainty in identifying the true measure of a quantity at the level of precision of the scale used for the quantity.

Algorithm

(AFOTTECP3)

A prescribed set of well-defined rules or processes for the solution of a problem in a finite number of steps.

Allocated Baseline

(AFR300-15)

The initial approved allocated configuration identification established at end of the definition phase.

Alternative

(ROWE)

One member of a set of options associated with a decision, the decision being limited to a choice of one and only one.

Application Functions

(AFOTTECP3)

Any functions which provide specific operational (mission) computations.

Application Software

(AFOTTECP5)

The software written by software support personnel, or purchased from a contractor, used directly in supporting ECSs. It is normally used for simulation, testing, and ECS code development.

Application Software (functional)

(AFR205X)

Those routines and programs designed by or for automatic data processing system users and customers to complete specific, mission-oriented task, jobs, or functions, using available automated data

processing equipment and basic software. Application Software may be either general purpose packages, such as demand deposit accounting, payroll, machine tool control, etc., or specific application programs tailored to complete a single or limited number of user functions (for example, base level personnel, depot maintenance, aircraft, missile or satellite tracking, command and control, etc.). Except for general purpose packages that are acquired directly from software vendors or from the original equipment manufacturers, this type of software is generally developed by the user, either with in-house resources or through contract services.

Approval to Operate

(AFR205X)

Represents concurrence by the designated approving authority (DAA) that a satisfactory level of security (that is, minimum requirements are met and an acceptable level of risk exists) has been provided, and authorizes the operation of an automated data processing system (ADPS) or network at an automatic data processing facility (ADPF). Approval results from an analysis of the ADPF, ADPS, and automatic data system (ADS) certifications and the operational environment of the automatic data processing (ADP) entity by the DAA.

Attributes

(AFOTEC3)

Type, units, range, description, etc., as appropriate.

Automated Decisionmaking System

(AFR205X)

Those computer applications which issue checks, requisition supplies, or perform similar functions based on programmed criteria, with little human intervention.

Automated Software Development Tool

(AFOTEC5)

A component of System Software that assists in the design, implementation, documentation, and verification of ECS software.

Automatic Data Processing Facility (ADPF)

(AFR205X)

The physical resources, including structures or parts of structures, which house and support data processing capabilities. For each computer facility designated as a data processing installation (DPI, reference AFR 300-6), the ADPF is the DPI. For small computers, stand-alone systems, and word processing equipment, the ADPF is the physical area in which the computer is used.

Automatic Data Processing Resources

(AFR205X)

The totality of automatic data processing equipment, software, data, computer time, computer programs, automatic data processing (ADP) contractual services, ADP personnel, and supplies.

Availability

(AFR800-14)

A measure of the degree to which an item is in the operable and committable state at the start of the mission, when the mission is called for at an unknown (random) point in time. (MIL-STD-721)

(AFOTECPS)

The probability that a system is operating satisfactorily at any point in time when used under stated conditions.

Baseline

(AFR300-15)

A configuration identification document or set of such documents formally designated and fixed at a specific time during a CPCI's life cycle. Baselines, plus approved changes to those baselines constitute the current configuration identification.

(ROWE)

A known reference used as a guide for further development activities.

Baseline Profile

(CURRENT)

The set of 27 pairs of numbers (or any subset) determined by specifying the (time to complete request, number of requests per unit time) pair for each maintenance request category.

Bayesian Statistics

(ROWE)

"Bayes Rule" (Thomas Bayes, a nineteenth century English mathematician and clergyman) states that the probability that both of two events will occur is the probability of the first multiplied by the probability that if the first has occurred, the second will also occur. Bayesian statistics is a way of making quantity of information substitute for quality of information. There are two kinds of probability: the classical type derived from empirical information,

and subjective probability. Bayesian statistics is based on these "subjective probabilities." It involves the joint probability of A and B. The probability of the second event occurring if the first has occurred is called the conditional probability of the second, given the first. Stated another way, the probability of any event $P(A)$ is always positive but never greater than 1. Symbolically, $0 \leq P(A) \leq 1$. If $P(A) = 0$, the occurrence of the event B is considered impossible. If $P(A) = 1$, the occurrence of the event B is considered to occur with $P(B)$.

Benefit

(ROWE)

- a) An axiological concept representing anything received that causes a net improvement to accrue to the recipient.
- b) A result of a specific action that constitutes an increase in the production possibilities or welfare level of society.

Benefit-Cost Ratio

(ROWE)

The ratio of total social benefit to total social costs related to a specific activity.

Capability

(ROWE)

A measure of the degree to which a system is able to satisfy its performance objectives.

Cardinal (interval) Scale

(ROWE)

A continuous scale between two end points, neither of which is necessarily fixed.

Complexity Level

(CURRENT)

The general degree of difficulty to complete a maintenance request: high, medium, low.

Computer Program

(AFR800-14)

A series of instructions or statements in a form acceptable to an electronic computer, designed to cause the computer to execute an operation or operations.

Computer Resources

(AFR800-14)

The totality of computer equipment, computer programs, associated documentation, contractual services, personnel and supplies.

Configuration Control

(AFR300-15)

The systematic evaluation, coordination, approval or disapproval, and implementation of approved changes in the configuration of a CPCI after formal establishment of its configuration identification.

Configuration Item (CI)

(AFR300-15)

An item of ADPE that is designated for configuration management.

(AFR800-14)

An aggregation of equipment/software, or any of its discrete portions, which satisfies an end use function and is designated by the Government for configuration management. CIs may vary widely in complexity, size and type, from an aircraft or electronic system to a test meter or round of ammunition. During development and initial production, CIs are only those specification items that are referenced directly in a contract (or an equivalent in-house agreement). During the operation and maintenance period, any reparable item designated for separate procurement is a configuration item.
(AFR 65-3)

Configuration Management (CM)

(AFR300-15)

A management discipline that applies technical and administrative direction and surveillance to:

- (1) Identify and document the functional and physical characteristics of a configuration item.
- (2) Control changes to those characteristics.
- (3) Record and report configuration status.

Configuration Management Plan (CMP)

(AFR300-15)

A document which describes project responsibilities and procedures for implementing CM.

Configuration Management System (CMS)

(AFOTEC P5)

A system applying technical and administrative direction and surveillance to identify and document the functional and physical

characteristics of a configuration item; to control changes to those characteristics and to record and report change processing and implementation status.

Consequence Value

(ROWE)

The importance a risk agent subjectively attaches to the undesirability of a specific risk consequence.

Consensus

(ROWE)

Group solidarity in sentiment and belief...general agreement.

Cost

(ROWE)

A result of a specific action that constitutes a decrease in the production possibilities or welfare level of society. Also see Loss.

Cost-Benefit Analysis

(ROWE)

An attempt to delineate and compare in terms of society as a whole the significant effects, both positive and negative, of a specific action. Generally a number of alternative actions are analyzed resulting in the selection of the alternative that provides either the largest benefit-cost ratio (total benefit/total cost) or one with a positive ratio at least. If an alternative results in a net benefit less than zero or a benefit-cost ratio less than 1, it is deemed socially inefficient and is not carried out.

Cost-Effectiveness Analysis

(ROWE)

A term less specific than cost-benefit analysis, usually meaning the selection of the lowest cost alternative that achieves a predetermined level of benefits. Alternatively, the analysis and selection of the path that yields the largest social benefit for a predetermined specified level of social costs.

Critical Automatic Data Processing Resources

(AFR205X)

Those resources that must be protected because their compromise, alternation, destruction, loss, or failure to meet objectives will jeopardize the accomplishment of an Air Force, Air Force subelement,

or other service mission or the accomplishment of DoD life support functions.

Critical Design Review (CDR)

(AFR300-15)

A formal review conducted during the development phase before translating logic, and algorithms to coded instructions.

Critical Issues

(AFOTECPI)

Those aspects of a system's capability, either operational, technical, or other, that must be questioned before a system's overall worth can be estimated and that are of primary importance to the decision authority in reaching a decision to allow the system to advance into the next acquisition phase. (DoD Directive 5000.3).

Data Item Description

(AFR800-14)

A form which specifies an item of data required to be furnished by a contractor. This form specifically defines the content, preparation instructions, format and intended use of each data product. (AFR 310-1)

Decision Analysis

(ROWE)

A methodology of decomposition of the decision-making process into parts, whereby the appropriate data can be associated with the parts, to provide a rational basis for decision making.

Decision Making

(ROWE)

A dynamic process of interaction, involving information and judgment among participants who determine a particular policy choice. Decision models are either models of the decision-making process itself, or analytical models (e.g., decision trees, decision matrices) used as aids in arriving at the decisions. Decision theories usually are in relation to the process itself.

Decision Matrices

(ROWE)

Matrices whose elements exhibit quantitative relationships (cardinal or ordinal) among sets of factors coming into play in the decision-making process.

Decision Tree

(ROWE)

A device used to portray alternative courses of action and relate them to alternative decisions showing all consequences of the decision. The tree represents alternative courses or series of actions related to a previous decision.

Decisive Decision Conditions

(ROWE)

Conditions in which the preference between values on a utility scale is clearly discernible because ranges of uncertainty of the two values do not overlap (in the case of uniform distributions of uncertainty) or are below a certain error level (for normal distributions of uncertainty).

Degree of Uncertainty

(ROWE)

That proportion of information about a total system that is unknown in relation to the total information about the system.

Delphi Technique

(ROWE)

An iterative method designed to produce a consensus by repeated queries of an individual with feedback of group responses. Members of the group do not interact directly.

Descriptive Uncertainty

(ROWE)

The absence of information about the completeness of the description of the degrees of freedom of a system.

Designated Approving Authority

(AFR205X)

An official designated to approve the operation of automatic data processing systems at the automatic data processing facilities under his or her jurisdiction for storage of classified or sensitive unclassified information or for critical processing.

Deviation

(AFR300-15)

A written authorization, granted prior to the development of a CPCI, to depart from a particular performance or design requirement; a

specification for a specific number of units; a specific period of time; or established standards.

Documentation

(AFOTECP5)

All of the written work describing operating and maintenance procedures for a system.

Documentation Consistency

(AFOTECP5)

A measure of the consistency in the information provided in support system documentation.

Documentation Descriptiveness

(AFOTECP5)

A measure of the descriptiveness of the information provided in support system documentation.

Documentation Modularity

(AFOTECP5)

A measure of the modular organization of information provided in support system documentation.

Documentation Simplicity

(AFOTECP5)

A measure of the ease of use and lack of complexity in the information provided in computer system documentation.

Embedded Computer Resources

(AFOTECP1)

Computer resources incorporated as integral parts of, dedicated to, required for direct support of, or for the upgrading or modification of major or less than major system(s). (Excludes ADP resources as defined and administered under AFR 300 series.) (USAF/RD/LE Policy letter, 13 October 1981).

Embedded Computer System (ECS)

(AFOTECP1)

a) A computer that is integral to an electromechanical system and that has the following key attributes:

- (1) Physically incorporated into a large system whose primary function is not data processing.

- (2) Integral to, or supportive of, a larger system from a design, procurement, and operations viewpoint.
 - (3) Inputs include target data, environmental data, command and control, etc.
 - (4) Outputs include target information, flight information, control signals, etc.
- b) In general, an embedded computer system (ECS) is developed, acquired, and operated under decentralized management. (DoD Directives 5000.1, 5000.2).

(AFOTEC P5)

A computer that is integral to an electronic or electromechanical system (e.g., aircraft, missile, spacecraft, communications device) from a design, procurement, and operational viewpoint.

Empirical

(ROWE)

Originating in or based on observation or experience.

Equitable Risk

(ROWE)

A risk agent receives direct benefits as a result of exposure to a risk, and the knowledge of the risk is not purposely withheld from the risk agent.

Estimation

(ROWE)

The assignment of probability measures to a postulated future event.

Estimator Uncertainty

(ROWE)

Uncertainty in measurement resulting from deliberate use of less complex measures such as central value estimates of dispersion and smoothing functions for time-dependent parameters.

Evaluation

(ROWE)

Comparison of performance of an activity with the objectives of the activity and assignment of a success measure to that performance.

Evaluation Criteria

(AFOTEC P1)

Standards by which achievement of required operational effectiveness/suitability characteristics or resolution of technical or

operational issues may be judged. For full-scale development and beyond, evaluation criteria must include quantitative goals (the desired value) and thresholds (the value beyond which the characteristic is unsatisfactory) whenever possible. (DoD Directive 5000.3).

Event

(ROWE)

A particular point in time associated with the beginning or completion of an activity, and possibly accompanied by a statement of the benefit or result attained or to be attained because of the completion of an activity.

Expandability

(AFOTECPS)

A measure of the ease with which the functional capability of computer hardware or software may be expanded.

Expected Value, Use Of

(ROWE)

Valuation of an uncertain numerical event by weighting all possible events by their probability of occurrence and averaging.

Expert Judgment

(ROWE)

Designating the relevance of opinions of persons well informed in an area for estimates (e.g., forecasts of economic activity).

Exposure (to risk)

(ROWE)

The condition of being vulnerable to some degree to a particular outcome of an activity, if that outcome occurs.

Extrapolation/Projection

(ROWE)

The technique of estimating the future by a continuation of past trends without attempts to understand the underlying phenomena.

Facility

(AFOTECPS)

The physical plant and the services it provides; specific examples are physical space, electrical power, physical and electromagnetic (TEMPEST) security, environmental control, fire safety provisions, and communications availability.

Feasible

(ROWE)

That which is possible to do, realistically.

Feedback

(ROWE)

The return of performance data to a point permitting comparison with objective data, normally for the purpose of improving performance (goal-seeking feedback), but occasionally to modify the objective (goal-changing feedback).

Firmware

(AFOTECPI)

- a) Computer programs and data loaded in a class of memory that cannot be dynamically modified by the computer during processing.
- b) Hardware that contains a computer program and data that cannot be changed in its application environment.

Note 1. The computer programs and data contained in firmware are classified as software; the circuitry containing the computer program and data is classified as hardware. (Data and Analysis Center for Software).

Functional Configuration Audit (FCA)

(AFR300-15)

The formal examination of CPCI to verify that the performance specified in the SS has been achieved.

Independent Verification and Validation (IV&V)

(AFOTECPI)

An independent assessment process structured to ensure that computer programs fulfill the requirements stated in system and subsystem specifications and satisfactorily perform the functions required to meet the user's and supporter's requirements. IV&V consists of three essential elements: independence, verification, and validation:

- (1) Independent. An organization/agency which is separate from the software development activity from a contractual and organizational standpoint.
- (2) Verification. The evaluation to determine whether the products of each step of the computer program development process fulfill all requirements levied by the previous step.
- (3) Validation. The integration, testing, and/or evaluation activities carried out at the system/subsystem level to

evaluate the developed computer program against the system specifications and the user's and supporter's requirements. (AFR 88-14)

Individual Risk Evaluation

(ROWE)

The complex process, conscious or unconscious, whereby an individual accepts a given risk.

Inequitable Risk

(ROWE)

A risk agent is exposed to a risk and receives no direct benefits from such exposure, or the knowledge of the risk is purposely withheld from him.

Interdependence

(ROWE)

A property shared by two or more entities whenever the performance of any one affects the performance of some or all the rest.

Interoperability

(AFOTTECP5)

A measure of the degree to which computer hardware or software can interface to and operate with other similar computer hardware or software.

Intrinsic Parameter

(ROWE)

A variable whose measurement is based on the value system of an individual and his perception of these values.

Loss Function

(ROWE)

A function used in decision theory for evaluating the losses incurred when certain decisions are made under uncertainty. If the loss function is independent of the decision value used, it is frequently called a cost function.

Maintainability

(AFOTTECP3)

Those characteristics of software which affect the ability of the software programmer to correct errors, enhance system capabilities

through software changes, and modify the software to be compatible with hardware changes.

(AFOTTECP5)

The probability that a system out of service for maintenance can be properly repaired and returned to service in a stated elapsed time.

Maintenance Documentation

(AFOTTECP5)

The documentation that describes the maintenance of computer system hardware and software.

Maintenance Request Category

(CURRENT)

The identification of a maintenance request by specification of the priority type, maintenance type, and complexity level.

Maintenance Type

(CURRENT)

The type of maintenance actions required to complete a maintenance request: enhancement, conversion, correction.

Measurable

(ROWE)

a) Capable of being sensed, that which is sensed being convertible to an indication; the indication can be logical, axiological, numerical, or probabilistic. If probabilistic, it is empirical and subjective.

b) Comparable to some unit designated as standard.

Measured Risk Level

(ROWE)

The historic, measured, or modeled risk associated with a given activity.

Measurement Uncertainty

(ROWE)

The absence of information about the specific value of a measurable variable.

Methodology

(ROWE)

An open system of procedures.

Model

(ROWE)

An abstraction of reality that is always an approximation to reality.

Module

(AFR300-15)

A program unit that is discrete and identifiable with respect to compiling and combining with other units.

Nominal Scale (taxonomy)

(ROWE)

A classification of items that can be distinguished from one another by one or more properties.

Objective Function

(ROWE)

A specified mathematical relationship between a dependent variable (e.g., overall measure of benefits) and a set of independent variables (e.g., individual benefit measures and their relative weights). In choosing among alternatives, the decision maker typically seeks to maximize the (dependent variable of the) objective function.

Operational Effectiveness

(AFOTECPl)

The overall degree of mission accomplishment of a system used by representative personnel in the context of the organization, doctrine, tactics, threat (including countermeasures and nuclear threats), and environment in the planned operational employment of the system. (DoD Directive 5000.3)

Operational Suitability

(AFOTECPl)

The degree to which a system can be satisfactorily placed in field use, with consideration being given availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, safety, human factors, manpower supportability, logistic supportability, and training requirements. (DoD Directive 5000.3)

Opinion Survey/Sampling

(ROWE)

Any procedure for obtaining by oral or written interrogation or both the views of any portion of the affected population regarding benefit levels expected, their utility, and/or relative importance. Typically, scientific sampling procedures would be used to maximize (for a given level of effort) the accuracy and precision of the results obtained.

Opportunity Cost

(ROWE)

The value to society of the next best alternative use of a resource. This is the true economic cost to society of using a resource for a specific purpose or in a specific project.

Ordinal Scale (rank scale)

(ROWE)

An ordering (ranking) of items by the degree to which they satisfy some criterion.

Paradigm

(ROWE)

A structured set of concepts, definitions, classifications, axioms, and assumptions used in providing a conceptual framework for studying a given problem.

Parametric Variation

(ROWE)

A technique for sensitivity analysis of any given model in which the values of parameters that are input to the model's calculation are systematically varied to permit observation of how such variation affects the model's output (especially ranking of alternatives).

Personnel

(AFOTECPS)

A general term for the experience, education, and quantity of people who are assigned to the software support facility either directly or indirectly maintaining the ECS. It includes Management, Technical, Support, and Contractor resources.

Personnel Profile

(AFOTECPS)

The characteristics that describe the experience, education, and quantity of software support facility personnel.

Physical Configuration Audit (PCA)

(AFR300-15)

The formal examination of the coded version of a computer program configuration item against its technical documentation.

Precision

(ROWE)

The exactness with which a quantity is stated; that is, the number of units into which a measurement scale of that quantity may be meaningfully divided. The number of significant digits is a measure of precision.

Predictive Modeling

(ROWE)

Use of any mathematic model that estimates or predicts the value of a dependent variable in terms of component factors specified as independent variables.

Preference

(ROWE)

Assignment of rank to items by an agent when the criterion used is utility to the ranking agent.

Priority Type

(CURRENT)

The criticality of the maintenance request in order to preserve mission readiness: emergency, urgent, normal.

Probability

(ROWE)

A numerical property attached to an activity or event whereby the likelihood of its future occurrence is expressed or clarified.

Probability Distribution

(ROWE)

The representation of a repeatable stochastic process by a function satisfying the axioms of probability theory.

Probability of Occurrence

(ROWE)

The probability that a particular event will occur, or will occur in a given interval.

Probability Threshold

(ROWE)

A probability of occurrence level for a risk below which a risk agent is no longer concerned with the risk and ignores it in practice (Threshold of concern).

Product Baseline

(AFR300-15)

The initial approved product configuration identification.

Product Verification Review (PVR)

(AFR300-15)

A formal review conducted by the developer for each CPCI at the end of the development phase to establish the Product Baseline for that CPCI and to ensure preparation for the Test Phase has been completed.

Program Manager

(AFR800-14)

The generic term used to denote a single Air Force manager (System Program Director, Program/Project Manager, or System/Item Manager) during any specific phase of the acquisition life cycle. (AFR 800-2).

Program Management Directive (PMD)

(AFR800-14)

The official HQ USAF management directive used to provide direction to the implementing and participating commands and satisfy documentation requirements. It will be used during the entire acquisition cycle to state requirements and request studies as well as initiate, approve, change, transition, modify or terminate programs. The content of the PMD, including the required HQ USAF review and approval actions, is tailored to the needs of each individual program. (AFR 800-2)

Program Management Plan (PMP)

(AFR800-14)

The document developed and issued by the Program Manager which shows the integrated time-phased tasks and resources required to complete the task specified in the PMD. The PMP is tailored to the needs of each individual program. (AFR 800-2)

Program Office (PO)

(AFR800-14)

The field office organized by the Program Manager to assist him in accomplishing the program tasks. (AFR 800-2)

Program Support Tools

(AFOTECP3)

General debug aids, test/retest software, trace software/hardware features, use of compiler/link editor, library management/configuration management/text editor/display software tools.

Program Test Plan

(AFOTECP3)

Set of descriptions and procedures for how the program is to be (or can be, or has been) tested.

Propensity for Risk Acceptance

(ROWE)

An individual, subjective trait designating the degree of risk one is willing to subject himself to for a particular purpose.

Quality Assurance (QA)

(AFR300-15)

All actions that are taken to assure that a development organization delivers products that meet performance requirements and adhere to standards and procedures.

Quantification

(ROWE)

The assignment of a number to an entity or a method for determining a number to be assigned to an entity

Reliability

(ROWE)

The probability that the system will perform its required functions under given conditions for a specified operating time.

Residual Risk

(AFR205X)

That portion of risk which remains after security measures have been applied.

Risk

(AFR205X)

The loss potential which exists as the result of threat/vulnerability pairs. Reducing either the threat or the vulnerability reduces the risk.

(ROWE)

The potential for realization of unwanted, negative consequences of an event.

Risk Acceptance

(ROWE)

Willingness of an individual, group, or society to accept a specific level of risk to obtain some gain or benefit.

Risk Acceptance Function

(ROWE)

A subjective operator relating the levels of probability of occurrence and value of a consequence to a level of risk acceptance.

Risk Acceptance Level

(ROWE)

The acceptable probability of occurrence of a specific consequence value to a given risk agent.

Risk Acceptance Utility Function

(ROWE)

The profile of the acceptability of the probability of occurrence for all consequences involved in a risk situation for a specific risk agent.

Risk Agent

(ROWE)

See Valuing Agent.

Risk Analysis

(AFR205X)

A part of risk management that is used to minimize risk by effectively applying security measures commensurate with the relative threats, vulnerabilities, and values of the resources to be protected. (The value of the resources includes impact on the organizations the automatic data processing system supports, and

impact of the loss or unauthorized modification of data). Risk analysis may be thought of as consisting of four modules: sensitivity assessment, risk assessment, economic assessment, and security test and evaluation.

Risk Assessment

(AFR205X)

A detailed study of the vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The results of a risk assessment may be used to develop security requirements and specifications.

(ROWE)

The total process of quantifying a risk and finding an acceptable level of that risk for an individual, group, or society. It involves both risk determination and risk evaluation.

Risk Averse

(ROWE)

Displaying a propensity against taking risks.

Risk Aversion

(ROWE)

The act of reducing risk.

Risk Baseline

(CURRENT)

The risk probability density function and the associated magnitude of consequence for the potential negative outcomes.

Risk Consequence

(ROWE)

The impact to a risk agent of exposure to a risky event.

Risk Conversion Factor

(ROWE)

A numerical weight allowing one type of risk to be compared to another type.

Risk Determination

(ROWE)

The process of identifying and estimating the magnitude of risk.

Risk Estimation

(ROWE)

The process of quantification of the probabilities and consequence values for an identified risk.

Risk Evaluation

(ROWE)

The complex process of developing acceptable levels of risk to individuals or society.

Risk Evaluator

(ROWE)

A person, group, or institution that seeks to interpret a valuing agent's risk for a particular purpose.

Risk Identification

(ROWE)

The observation and recognition of new risk parameters, or new relationships among existing risk parameters, or perception of a change in the magnitude of existing risk parameters.

Risk Management

(AFR205X)

The total process of identifying, controlling, and minimizing uncertain events. The process of obtaining and maintaining DAA approval is a major element of the risk management program. The process facilitates the management of automatic data processing (ADP) security risks by each level of ADP management throughout the ADP life cycle. The approval process consists of three elements: risk analysis, certification, and approval.

Risk Profile Baseline

(CURRENT)

The measure of information and/or requirements which serve as the zero reference against which negative (and positive) outcomes can be determined.

Risk Proportionality Derating Factor

(ROWE)

Quantifying the degree to which risks become less acceptable as indirect benefits to the risk agent declines.

Risk Proportionality Factor

(ROWE)

That portion of the total societal risk that society will accept for a new technology.

Risk Reduction

(ROWE)

The action of lowering the probability of occurrence and/or the value of a risk consequence, thereby reducing the magnitude of the risk.

Risk Reference

(ROWE)

Some reference, absolute or relative, against which the acceptability of a similar risk may be measured or related; implies some overall value of risk to society.

Risk Referent

(ROWE)

A specific level of risk deemed acceptable by society or a risk evaluator for a specific risk; it is derived from a risk reference.

Risky Shift

(ROWE)

The tendency of certain groups to become more extreme or take riskier positions in their judgments than they would acting as individuals.

Sensitivity Analysis

(ROWE)

A method used to examine the operation of a system by measuring the deviation of its nominal behavior due to perturbations in the performance of its components from their nominal values.

Simulation

(AFR800-14)

The representation of physical systems or phenomena by computers, models or other equipment.

Software

(AFOTECPI)

A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system.

(CURRENT)

The programs which execute in a computer. The data input, output, and controls upon which program execution depends and the documentation which describes, in a textual medium, development and maintenance of the programs.

Software Error

(CURRENT)

The human decision (inadvertent or by design) which results in the inclusion of a fault in a software product.

Software Fault

(CURRENT)

The presence or absence of that part of a software product which can result in software failure.

Software Maintainability

(AFOTECPI)

The ease with which software can be changed in order to:

- (1) Correct errors.
- (2) Add or modify system capabilities through software changes.
- (3) Delete features from programs.
- (4) Modify software to be compatible with hardware changes.

(CURRENT)

A quality of software which reflects the effort required to perform software maintenance actions.

Software Maintenance

(CURRENT)

Those actions required for:

- (1) Correction. Removal, correction of software faults
- (2) Enhancement. Addition/deletion of features from the software
- (3) Conversion. Modification of the software because of environment (data hardware) changes.

Software Maintenance Environment

(CURRENT)

An integration of personnel support systems and physical facilities for the purpose of maintaining software products.

Software Maintenance Measures

(CURRENT)

Measures of software maintainability and environment capabilities to support software maintenance activity.

Software Management

(CURRENT)

The policy, methodology, procedures, and guidelines applied in a software environment to the software development/maintenance activities. Also, those personnel with software management responsibilities.

Software Reliability

(CURRENT)

A quality of software which reflects the probability of failure free operation of a software component or system in a specified environment for a specified time.

Software Portability

(CURRENT)

A quality of software which reflects the effort required to transfer the software from one environment (hardware and system software) to another.

Software Support Facility (SSF)

(AFOTECPS)

The facility which houses and provides services for the support systems and personnel required to maintain the software for a specific ECS.

Software Supportability

(CURRENT)

A measure of the adequacy of personnel, resources, and procedures to facilitate:

- (1) Modifying and installing software
- (2) Establishing an operational software baseline
- (3) Meeting user requirements.

Software Supportability Evaluation Metrics

(CURRENT)

The closed-form questionnaire scores for each characteristic and cumulated level in a software supportability evaluation.

Software Supportability Magnitude of Risk Consequence

(CURRENT)

The level of impact to a software user or supporter as a result of the risk level of a software supportability negative outcome.

Software Supportability Negative Outcome.

(CURRENT)

The final result of a maintenance request as represented by the pair (time to complete request, number of requests per unit time), in which the Baseline SS Profile is not met.

Software Supportability Risk Agent Acceptance Level

(CURRENT)

The software supportability risk level which is acceptable to a risk agent.

Software Supportability Risk Level.

(CURRENT)

The potential for realization of a software supportability negative outcome.

Specification

(AFR300-15)

A document that describes the requirements for the development or acquisition of ADPE and/or software.

Standards

(AFOTECP3)

Procedures, rules, and conventions used for prescribing disciplined program design and implementation.

States of Nature

(ROWE)

A concept from decision theory. In decision making under uncertainty, the outcomes (numerical results) associated with each available alternative are considered to be predictable as a set of n discrete values depending on conditions beyond the decision maker's control and for which he has no useful estimates of the respective probabilities. The n sets of conditions under which each one of the outcomes is expected are termed "states of nature."

Structured Value (structured value analysis)

(ROWE)

The resultant value of a particular value set evaluated for a particular data set. This value lies between zero and unity and allows many data sets to be ranked numerically in relation to one another.

Structured Value Analysis

(ROWE)

A multistage procedure for assessing the value of an action, project alternative, and so on, incorporating individual techniques at each stage for computing from quantitative measures of individual components a single figure expressing the overall value. A multistage procedure for assessing the value of an action, project, alternative, and so on, by structuring the complete entity into component elements, to each of which a numeric measure of value (positive or negative) can be assigned. These are then converted to a common utility scale. Each component is assigned a weight expressing its relative significance in determining overall value of the entity. A single figure of worth or value is then computed from measures and weights of all individual components. The procedure permits considerable flexibility in choice of techniques used to perform each necessary optimal step.

Subjective Probabilities

(ROWE)

The assignment of subjective weights to possible outcomes of an uncertain event where weights assigned satisfy axioms of probability theory.

Support Personnel

(AFOTECPS)

A general term for military or DoD civilian personnel whose skills are necessary for the software support facility to function but who do not directly support ECS software maintenance.

Support System

(AFOTECPS)

Any automated system used to change, test, or manage the configuration of ECS software and associated documentation. Includes but is not limited to Host Processor, Software Bench, Laboratory-Integrated Test Facility, Operational-Integrated Test Facility, and Configuration Management System.

Support System Facility

(AFOTEC P5)

The facility resources that must be available for the software support resources to accomplish a specific task(s) (see General Facility).

Surrogate or Proxy Measures

(ROWE)

The use of a related quantity as a proxy for an unknown or difficult-to-measure value. The relationship may be established by arm-chair analysis, correlation techniques, scientific studies, or other means.

System

(ROWE)

a) A complex entity formed of many, often diverse, parts subject to a common plan or serving a common purpose.

b) A composite of equipment, skills, and techniques capable of performing and/or supporting an operation.

System Design Review (SDR)

(AFR300-15)

A formal review of the system design approach for an ADS.

System Requirements Review (SRR)

(AFR300-15)

A formal review of the requirements for an ADS.

System Software

(AFOTEC P5)

All of the software that is part of the software support facility computer system. It is never or seldom accessed directly by software support facility personnel; it controls the processing of application software. It includes the Operating System, Source Code Editor, Language Translator, Link Editor/Loader, Librarian/File Manager, Data Base Manager, and Automated Software Development Tool.

Taxonomy

(ROWE)

The identification and definition of properties of elements of the universe; a disaggregation, as contrasted with systematics (which is an aggregation) and as contrasted with morphology (which encompasses both taxonomy and systematics).

Test Analysis Report (RT)

(AFR300-15)

A document containing the results and analyses of tests executed during the Test Phase.

Threshold

(ROWE)

A discontinuous change of state of a parameter as its measure increases. One condition exists below the discontinuity, and a different one above it.

Time to Complete Maintenance Request (TC)

(CURRENT)

The calendar time from receipt of the maintenance request by the support control group until the request has been denied or the maintenance actions required by request have been accepted as part of an operational system software configured release. (This does not mean the configuration is released or distributed, and this time does not include this additional delay if any.)

Transfer

(AFR800-14)

That point in time when the designated Supporting Command accepts program management responsibilities from the Implementing Command. This includes logistic support and related engineering and procurement responsibilities. (AFR 800-4)

Turnover

(AFR800-14)

That point in time when the operating command formally accepts responsibility from the Implementing Command for the operation and maintenance of the system, equipment, or computer program acquired. (AFR 800-19)

Uncertainty

(ROWE)

The absence of information; that which is unknown.

User

(AFR205X)

Any persons (or organizations) having access to an automatic data processing system via communication through a remote device or who

is allowed to submit input to the system through other media (for example, tape or card decks). (Does not include those persons or organizations defined as customers.)

Valuation

(ROWE)

The act of mapping an ordinal scale onto an interval scale i.e., assigning a numerical measure to each ranked item based on its relative distance from the end points of the interval scale... assigning an interval scale value to a risk consequence.

Value

(ROWE)

A quality quantified on a scale expressing the satisfaction of man's intrinsic wants and desires.

Value Function (structured value analysis)

(ROWE)

A function relating points on the parameter measurement scale to the value scale for a particular parameter. These functions may result from explicit information or may be arrived at through value judgment.

Value Set (structured value analysis)

(ROWE)

A specific set of model parameters made up of terms and factors, expressed in particular measurement scales, value functions, and weights.

Valuing

(ROWE)

The act of assigning a value to a risk consequence.

Valuing Agent

(ROWE)

A person or group of persons who evaluates directly the consequence of a risk to which he is subjected. A risk agent.

Verification/Validation (of computer programs)

(AFR800-14)

The process of determining that the computer program was developed in accordance with the stated specification and satisfactorily performs, in the mission environment, the function(s) for which it was designed.

Weight (structured value analysis)

(ROWE)

The relative importance of terms in a model expressed as a decimal fraction; weights for a set of terms add to unity.

Weighting Factor

(ROWE)

A coefficient used to adjust variable accuracy to a subjective evaluation; these factors are usually determined through surveys, Delphi sessions, or other formats of expressing social priorities.