

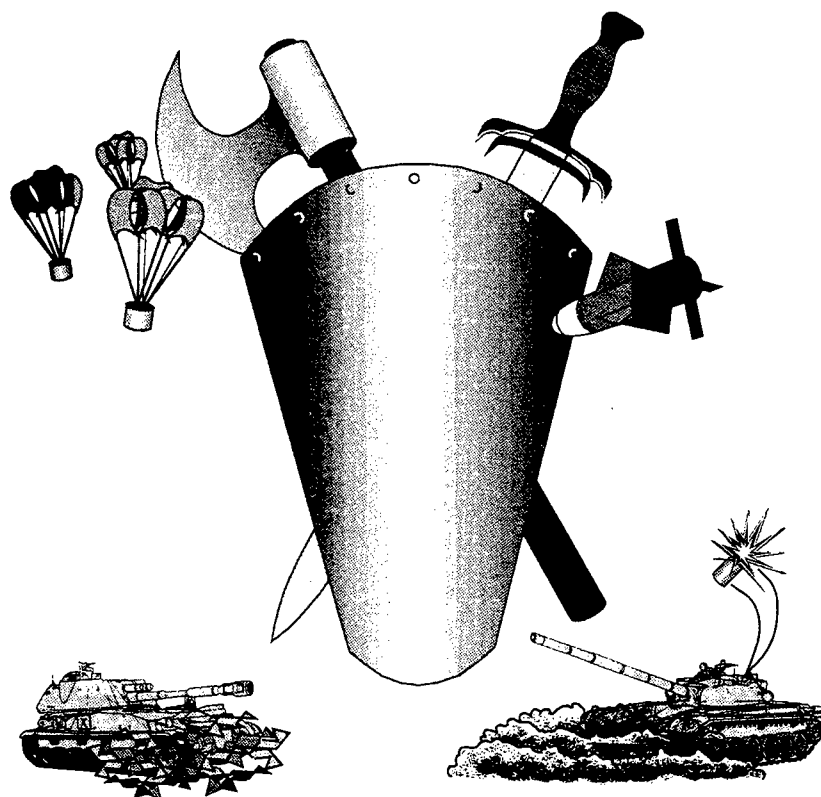
GACIAC

GUIDANCE & CONTROL
INFORMATION ANALYSIS CENTER

GACIAC SR-93-01

AMC-SWMO COUNTERMEASURES STUDY

*Volume IV: Guide to Army Smart Weapons
Testing Issues*



19990604 033

Published by GACIAC
IIT Research Institute
10 West 35th Street
Chicago, IL 60616-3799

FOURTH PRINTING
JUNE 1993

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

NOTICES

Special Report. This special report has been published by the Guidance and Control Information Analysis Center (GACIAC) as a service to the defense community. GACIAC is a DoD Information Analysis Center, administered by the Defense Technical Information Center, operated by IIT Research Institute under Contract No. DLA-900-86-C-0022. GACIAC is funded by DTIC, DARPA and U.S. Army, U.S. Navy, and U.S. Air Force Laboratories/Controlling Activities having an interest in weapon guidance and control. The Director of GACIAC is Dr. Robert J. Heaston. The Contracting Officer is Ms. Cheryl Montoney, DESC, Dayton, Ohio. The Contracting Officer's Technical Representative is Mr. Chalmer D. George, and the Alternate Representative is Mr. H.C. Race, U.S. Army Missile Command, AMC Smart Weapons Management Office, Attn: AMSMI-SW, Redstone Arsenal, Alabama 35898-5222.

Reproduction. Permission to reproduce any material contained in this document must be requested from and approved in writing by the U.S. Missile Command, AMC Smart Weapons Management Office, Attn: AMSMI-SW, Redstone Arsenal, Alabama 35898-5222. This document is only available from GACIAC, IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799. Copies are available to Government agencies under service supplementary core funding and GACIAC industrial subscribers. Cost to others as indicated in block 16 of the inclosed Standard Form 298 (page i), are authorized to offset reproduction and distribution costs by GACIAC.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information including suggestions for reducing the burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE Reprinted June 1993		3. REPORT TYPE AND DATES COVERED Special Report; 19 June 1989
4. TITLE AND SUBTITLE AMC-SWMO Countermeasures Study; Volume IV: Guide to Army Smart Weapon Testing Issues			5. FUNDING NUMBERS DLA900-86-C-0022 PE 65805	
6. AUTHOR(S) Jim Otto				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) IIT Research Institute/GACIAC 10 West 35th Street Chicago, IL 60616-3799			8. PERFORMING ORGANIZATION REPORT NUMBER GACIAC SR-93-01 Volume IV	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) US Army Missile Command AMC Smart Weapons Management Office Attn: AMSMI-SW Redstone Arsenal, AL 35898-5222			10. SPONSORING/MONITORING AGENCY REPORT NUMBER AD-E-951-925	
11. SUPPLEMENTARY NOTES This document is available only from GACIAC, IIT Research Institute, 10 West 35th Street, Chicago, IL 60616-3799. (410948)				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.			12b. DISTRIBUTION CODE "A"	
13. ABSTRACT (Maximum 200 words) This volume "Guide to Army Smart Weapon Testing Issues" is a primer intended basically for the development engineers in the smart weapon program management offices who are responsible for organizing smart weapon development tests. Much of the information in this guide is relevant to the ground vehicle developer. The document examines a number of issues, suggestions, and general principles pertinent to smart weapon testing. The information contained in this document is based on numerous interviews with experienced Army smart weapon testers.				
14. SUBJECT TERMS Smart weapons, Smart sensors, Precision guided munitions, Countermeasures, Testing, Test and evaluation, Field tests, Simulation, Computerized simulation, Test plan, Test facilities, Handbooks.			15. NUMBER OF PAGES 108	
			16. PRICE CODE \$50	
17. SECURITY CLASSIFICATION OF REPORT Unclassified/Unlimited	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unclassified	

AMC-SWMO COUNTERMEASURES STUDY

Volume IV: Guide to Army Smart Weapons Testing Issues

**Approved for Public Release:
Distribution Unlimited**

Published by GACIAC
IIT Research Institute
10 West 35th Street
Chicago, Illinois 60616-3799

**FOURTH PRINTING
JUNE 1993**

*GACIAC - A DoD Information Analysis Center
Operated by IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799
DoD Technical Sponsor-Joint Service Guidance and Control Committee
Members from OSD, Army, Navy, Air Force and DARPA*

FOREWORD

This "Guide to Army Smart Weapon Testing Issues" is a primer intended primarily for the development engineers in the smart weapon program management offices who are responsible for organizing smart weapon developmental tests. Much of the information in this guide is also relevant to the ground vehicle developer. The document examines a number of issues, suggestions, and general principles relevant to smart weapon testing. The information contained in this document is based primarily on numerous interviews with experienced Army smart weapon testers.



Just as the conductor of an orchestra follows the composer's musical score to achieve a desired impact on a specific audience, a test conductor must execute a test founded on a comprehensive, coordinated, and criteria-driven test plan that meets the decision makers' requirements for

information. The analysis of the data is no better than the plan.

In smart weapons employment (testing), there is no such thing as a "benign target in a sterile environment"! Therefore, all smart weapons testing must be considered with varying degrees of CMs present.

Howard C. Race

Howard C. Race
Technical Director and Deputy Director
AMC-Smart Weapons Management Office

PREFACE

The Army Materiel Command Smart Weapons Management Office (AMC-SWMO) has prepared a series of publications defining CM/CCM robustness assessment methodology, which they would like to make available to a broader audience. Three publications are involved:

- AMC-SWMO Countermeasures Study, Volume I:
Guide to How Countermeasures Affect Smart Weapons
(Unclassified/Unlimited)
- AMC-SWMO Countermeasures Study Volume II:
Effects of Countermeasures on Smart Weapons Technology
(Secret)
- AMC-SWMO Countermeasures Study, Volume IV:
Guide to Army Smart Weapon Testing Issues
(Unclassified/Unlimited)

These three volumes are being reprinted by the Guidance and Control Information Analysis Center (GACIAC) at the request of SWMO. All three are being published as separate volumes of a GACIAC Special Report (SR) which is numbered GACIAC SR-93-01. Each of the volumes was prepared by different authors; their results are being published as released by AMC-SWMO.

There is a Volume III in this countermeasures series but it is classified and is for controlled distribution (by permission only). Volume III discusses countermeasures against five specific weapon systems and contains an Executive Summary of the overall AMC-SWMO Countermeasures Study. The five systems discussed under Volume III are:

- Vol III-A: Sense & Destroy Armor (SADARM) (Secret)
- Vol III-B: Smart Target Activated Fire and Forget (STAFF) (Secret/NF)
- Vol III-C: Non-Line of Sight Anti-Tank (NLOS-AT) (Secret/NF)
- Vol III-D: MLRS-Terminal Guidance Warhead (MLRS-TGW) (Secret)
- Vol III-E: Generic LADAR Anti-Armor System (GLAAS) (Secret)

If anyone would like more details on Volume III, please contact the GACIAC Contracting Officers Technical Representative (COTR) at the following AMC-SWMO address:

Commander
US Army Missile Command
Attn: AMSMI-SW (Chalmer D. George)
Redstone Arsenal, AL 35898-5222

Dr. Robert J. Heaston
Director of GACIAC

EXECUTIVE SUMMARY

The basic purpose of this document is to provide a primer on the general principles and issues relevant to the management, planning and implementation of Army smart weapon (SW) testing. This "Guide to Army Smart Weapon Testing Issues" is intended primarily for the development engineers in the smart weapon program management offices who are responsible for organizing smart weapon developmental tests. This volume covers aspects of both developmental testing (DT) and operational testing (OT). Its focus is on developmental testing, although many of the issues and principles apply to both DT and OT.

Smart weapon testing can present unique challenges to the tester. First, SW performance is sensitive to its surrounding environment. This can generate the need to test and evaluate SWs under many conditions and requires the tester to thoroughly quantify the environment. Second, SWs involve a number of complex subsystems that must work together to make decisions and autonomously engage a target. This may require that these subsystems be extensively tested individually to fully characterize the various subsystems' performance. Third, some types of SWs are many-on-many systems (many submunitions engaging many targets). This can require unique and extensive test instrumentation and resources that are capable of collecting the appropriate test data on many submunitions simultaneously engaging many targets. This guide discusses these issues and presents some testing principles that address them. These principles are outlined below.

Plan, plan, and plan again: SW testing is an expensive and complicated endeavor. Detailed and early test planning and coordination at all levels (TEMP, individual testing, etc.) can help make the testing run more efficiently and smoothly. There are two basic levels of test planning. The more general level of test planning outlines what tests should occur, when they should occur, and what their primary objectives

should be. This higher level planning is primarily the function of the program manager (PM) and a variety of organizations interacting via the Test Integration Working Group (TIWG)--the results of which are addressed in the Test and Evaluation Master Plan (TEMP). The more detailed type of test planning involves the specific arrangements necessary to carry out a particular test --the results of which are summarized in the Detailed Test Plan (DTP). The basic activities involved in planning a typical SW test can be summarized as: Establishing the Test Planning Organization; Defining the Test Data Requirements and Test Matrix; Specifying and Arranging for Test Resources; and Generating and Coordinating the DTP.

Beware the Long Lead Item: Long lead items can cause unexpected problems and must be carefully managed. Some specific long lead items associated with SW testing include range clearances, test resources, target validation, and radio frequency allocations.

Validate Your Targets: To be suitable for SW testing, threat targets must be validated and accredited. This authentication process is required because the characteristics of a test target can strongly impact the performance of a SW. The Project Manager for Instrumentation, Targets, and Threat Simulators (PM ITTS) can provide help in procuring or developing targets. The validation process falls under the purview of a Validation Working Group (VWG) which authors the Target Validation Report. Target accreditation is the responsibility of the Target Accreditation Working Group (TAWG), which authors the Target Accreditation Report.

Get Your Countermeasures Blessed: It is important to work closely with the intelligence community to sanction the CMs to be used in a test. General information and requirements concerning CMs that need to be tested are contained in the System Threat Assessment Report (STAR) and other documented sources of validated threat information for the SW of interest. The Vulnerability Assessment Laboratory (VAL) and other relevant intelligence sources such as the local Foreign Intelligence Office

(FIO), the Foreign Science and Technology Center (FSTC) and the Missile Space Intelligence Center (MSIC) can provide more detailed guidance and interpretation.

Integrate Testing and Simulation: The generally accepted approach to system evaluation used to be that simulation and developmental testing were conducted to generate the data needed to develop the system. Operational testing, on the other hand, was conducted as essentially a pass/fail test after the system was developed. DT and OT were generally conducted independently of one another. However, because of testing and funding constraints, this previous approach has been evolving to a new strategy where DT, OT, and simulation results are all used to form an integrated picture of SW performance. While testing is generally much more costly than simulation, testing results usually have more credibility than simulation data. Simulations, on the other hand, are much more flexible and cost effective and can be used to extrapolate test data and to support test planning.

Work With Your Operational Tester: In the past, the operational tester started testing as the system was nearing production. However, as systems become more complex, test requirements increase, and test resources become harder to get, it is inevitable that DT and OT will start concurrently. The obvious advantage to combined DT and OT is in conserving test resources. There are also some disadvantages to conducting concurrent DT and OT. Most importantly, the DT and OT objectives may conflict (DT usually wants a lot of data under controlled conditions, whereas OT usually wants limited data under uncontrolled conditions.). The process of accommodating both DT and OT objectives in the same test is one of negotiation and compromise.

Maintain Strong Control During Testing: During testing, it is important to maintain a strong grasp on what is happening and to stick to the test plan. Any changes to testing must be carefully controlled, but flexibility is needed in DT. Changes must first be fully deliberated and reflected in the test matrix before being implemented. The

test director should have at least daily coordination meetings during the test to coordinate test matrix changes and other issues. It is important to keep good records during testing, to include good ground truth data and an efficient quick-look analysis and database capability.

Work With Your Data Analyst: Good communications should be fostered between the people taking the test data and those who will use it. Both the analysts and testers should work together to generate the test matrix. The analysts are the best ones to know what data they need and in what format. The testers can apply a measure of practicality to the analysts' requests. This strategy also fosters an integrated approach to SW evaluation.

Collect Good Ground Truth Data: Because SW systems can be strongly affected by their operating environment, it is important that the critical environmental parameters be recorded properly. Without the appropriate ground truth data, it may not be possible to properly analyze the test data results. Ground truth data is very important for DT search, detection and tracking tests. Ground truth data should be collected at the same time, location, spectral band, and boresight of the system of interest. Another important consideration when collecting ground truth is the effect that the CMs will have on the ground truth instrumentation. It doesn't make much sense to try and collect ground truth data with instrumentation that will be made inoperable by the CMs.

These principles of SW testing provide a good framework for implementing a SW test. In addition to these ideas, this guide also lists a number of references and points of contact that can be accessed to provide guidance in planning, coordinating and implementing a SW test.

TABLE OF CONTENTS

FOREWORD	ii
EXECUTIVE SUMMARY	iii
TABLE OF CONTENTS	vii
LIST OF FIGURES	viii
LIST OF TABLES	viii
LIST OF ABBREVIATIONS/ACRONYMS	ix
1.0 INTRODUCTION	1-1
2.0 SMART WEAPON TESTING ISSUES AND PRINCIPLES	2-1
2.1 Plan, Plan, and Plan Again	2-5
2.1.1 Establish the Test Planning Organization	2-14
2.1.2 Develop Test Data Requirements	2-16
2.1.3 Define Test Conditions	2-19
2.1.4 Specify and Arrange for Required Test Resources and Clearances	2-23
2.1.5 Generate and coordinate the Detailed Test Plan	2-26
2.2 Beware the Long Lead Item	2-29
2.3 Validate Your Targets	2-32
2.4 Get Your Countermeasures Blessed	2-36
2.5 Integrate Testing and Simulation	2-39
2.6 Work With Your Operational Tester	2-43
2.7 Maintain Strong Test Controls	2-45
2.8 Work With Your Data Analyst	2-47
2.9 Collect Good Ground Truth Data	2-48
3.0 SUMMARY	2-50
APPENDIX A: U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets	A-1
APPENDIX B: Detailed Test Plan Outline	B-1
REFERENCES	R-1

LIST OF FIGURES

Figure 2-1	Detailed Test Plan	2-9
Figure 2-2	Test Management Team Organization	2-14
Figure 2-3	Common Types of Smart Weapon Countermeasures	2-20
Figure 2-4	Test Resources and Clearances	2-24
Figure 2-5	Intelligence Agencies	2-37
Figure 2-6	Approach to DT and OT	2-40

LIST OF TABLES

Table 1-1	Army Agencies Consulted	1-2
Table 2-1	Project File Content	2-16
Table 2-2	Example Test Matrix	2-17
Table 2-3	Typical Ground Truth Data	2-18
Table 2-4	Target Conditions	2-19
Table 2-5	Common Countermeasure Technical Parameters	2-21
Table 2-6	Environmental Factors	2-18
Table 2-7	Potential SW CM Test Sites	2-25
Table 2-8	Suggested Detailed Test Plan Outline	2-26
Table 2-9	DTP Considerations	2-27

List of Abbreviations/Acronyms

ABM	Anti-Ballistic Missile
ACRV	Armored Combat Reconnaissance Vehicle
ADP	Automatic Data Processing
ADTC	Armament Development and Test Center
AFB	Air Force Base
AFMIC	Army Foreign Medical Intelligence Center
AM	Amplitude Modulation
AMC	Army Materiel Command
AMSAA	Army Materiel Systems Analysis Activity
AR	Army Regulation
ARDEC	Armament Research, Development and Engineering Center
ARMTE	Army Materiel Test and Evaluation
ARL	Army Research Laboratory (replaced LABCOM)
ASAT	Anti-Satellite
ATGM	Anti-Tank Guided Missile
BW	Biological Warfare
CCM	Counter-Countermeasure
CEP	Circular Error Probable
CFT	Captive Flight Test
CG	Commanding General
CI	Counter-Intelligence
CM	Countermeasure
COMM	Commercial
CRTC	Cold Regions Test Center
CSTA	Combat Systems Test Activity
CW	Chemical Warfare
CYA	Confirm your assessments
DA	Department of the Army
DAAT	Data Acquisition and Analysis Team
DCSINT	Deputy Chief of Staff, Intelligence
DEV	Development
DEW	Directed Energy Weapon
DIA	Defense Intelligence Agency
DOD	Department of Defense
DSN	Defense Switched Network
DT	Developmental Testing
DTP	Detailed Test Plan
EMD	Engineering and Manufacturing Development
EMI	Electro-Magnetic Interference
EOD	Explosive Ordnance Disposal

List of Abbreviations/Acronyms (continued)

EW	Electronic Warfare
FIO	Foreign Intelligence Office
FLIR	Forward Looking Infrared
FM	Frequency Modulation
FME	Foreign Materiel Exploitation
FMP	Foreign Military Production
FS	Fire Support
FSTC	Foreign Science & Technology Center
GACIAC	Guidance and Control Information Analysis Center
HPM	High Power Microwave
HQDA	Headquarters, Department of the Army
HWIL	Hardware in the Loop
IEP	Independent Evaluation Plan
IMINT	Image Intelligence
INTEL	Intelligence
IR	Infrared
ITAC	Intelligence Threat Analysis Center
ITTS	Instrumentation, Targets and Threat Simulators
JPG	Jefferson Proving Ground
LOS	Line of Sight
LWIR	Long Wave Infrared
MICOM	Missile Command
MLRS-TGW	Multiple Launch Rocket System-Terminal Guidance Warhead
MMW	Millimeter Wave
MNS	Mission Need Statement
MS	Milestone
MSC	Major Subordinate Command
MSIC	Missile Space Intelligence Center
MTLB	CIS light reconnaissance vehicle
MWIR	Mid-Wave Infrared
N ₂	Nitrogen
NASA	National Aeronautics and Space Administration
NWC	Naval Weapons Center
OPTEC	Operational Test and Evaluation Command
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT	Operational Testing
OTD	Office of the Test Directorate
P ³ I	Preplanned Product Improvement
P _d	Probability of Detection

List of Abbreviations/Acronyms (continued)

PDF	Probability Density Function
PEO	Program Executive Officer
PFRR	Poker Flats Research Range
PM	Program Manager or Project Manager
PQT	Production Qualification Test
PSD	Power Spectral Density
RAM	Radar Absorbing Material
RCR	Radar Corner Reflector
RCS	Radar Cross Section
RD&EC	Research, Development and Engineering Center
RF	Radio Frequency
RTTC	Redstone Technical Test Center
SADARM	Sense and Destroy Armor
SAM	Surface to Air Missile
SEMI	Special Electro-Magnetic Interference
SIGINT	Signals Intelligence
SIM	Simulation
SMO	Survivability Management Office
SOMTE	Soldier-Operator-Maintainer, Test and Evaluator
SRBM	Short Range Ballistic Missile
STAR	System Threat Assessment Report
STU-III	Secure Terminal Unit
SW	Smart Weapon
SWIR	Short Wave Infrared
SWMO	Smart Weapon Management Office
T&E	Test and Evaluation
TAWG	Target Accreditation Working Group
TDP	Test Design Plan
TECOM	Test and Evaluation Command
TEMA	Test and Evaluation Management Agency
TEMP	Test and Evaluation Master Plan
TFT	Technical Feasibility Tests
TISO	Threat Intelligence Staff Officer
TIWG	Test Integration Working Group
TMT	Test Management Team
TOW	Tube-Launched, Optically-Tracked, Wire-Guided
TRADOC	Training and Doctrine Command
TTR	Tonopah Test Range
TTSP	Threat Test Support Plan
UTTR	Utah Test and Training Range

List of Abbreviations/Acronyms (continued)

VAL	Vulnerability Assessment Laboratory
VLAMO	Vulnerability Lethality Assessment Management Organization
VWG	Validation Working Group
WSMR	White Sands Missile Range
YPG	Yuma Proving Ground

1.0 INTRODUCTION

The basic purpose of this document is to provide a primer on the general principles and issues relevant to the management, planning and implementation of Army smart weapon (SW) testing. It is important that the reader understand, up front, the perspective of this report. There are a large number of different types of tests that occur throughout the system life cycle (See References 1, 9 and 18 for detailed discussions of the different types of testing). This guide focuses on developmental testing (versus operational or other type testing) and emphasizes performance field testing (versus laboratory testing such as climatic or reliability testing). This guide includes SW testing issues related to the developmental testing that is performed to collect the test data necessary to 1) conduct engineering and manufacturing development and 2) test system performance against user requirements. This said, many of the issues related to developmental testing will also be relevant to operational testing.

This primer is intended primarily for the development engineers who are responsible for planning and implementing technical developmental tests for SW program management offices. It provides a number of issues and general principles relevant to SW testing based primarily on numerous interviews with experienced Army SW testers.

The basic approach in developing this guide has been a simple one. It is recognized that detailed testing knowledge does not generally reside in

Army Regulations or in Technical Manuals. While these types of documents are useful, they are generally broad and top level and outline policy and coordination approval processes. The more specific information on test planning and execution

**Call Brian Matkin to comment:
DSN: 788-8912
COMM: (205) 842-8912**

techniques resides in the experience and expertise of practiced testers in the field. For this reason, interviews were conducted with numerous experienced testers in a number of different Army agencies (See Table 1-1). This document is intended to capture some of their expertise and knowledge. It is realized that many others may also have valuable information relevant to this handbook. This should be a living document--comments can be provided to Brian Matkin at DSN: 788-8912 or COMM: (205) 842-8912. There is also a comment form at the back of the document that can be mailed in.

Table 1-1 Army Agencies Consulted

- Chicken Little Joint Program Office
- AMC Smart Weapons Management Office
- PEO Tactical Missiles
- PM MLRS-TGW
- PM Javelin
- Redstone Technical Test Center (RTTC)
- WSMR Instrumentation Directorate (ID)
- Vulnerability Assessment Lab (VAL)
- DoD Office of the Test Directorate (OTD)
- WSMR National Range Operations
- Army Materiel Test and Evaluation (ARMTE)
- Foreign Science & Technology Ctr (FSTC)
- PM Instr, Targets & Threat Simulators (PM ITTS)
- HQ DA DCSINT (HQDA Intelligence)
- PM SADARM

2.0 SMART WEAPON TESTING ISSUES AND PRINCIPLES

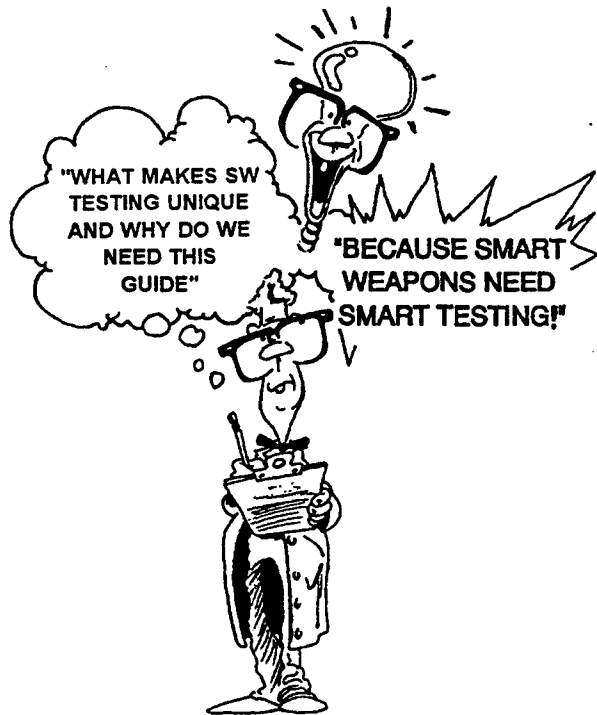
Smart weapon testing can present many unique challenges to the tester. There are several reasons for this.

First, SW performance is sensitive to its surrounding environment. This can generate the need to test and evaluate SWs under many conditions and requires the tester to thoroughly quantify the environment.

SWs are complex systems that interact with, and are impacted by, the environment and scenario in which they operate. This is primarily because they must make autonomous decisions based on their perception of the surroundings.

These complicated interactions with the environment can strongly affect the performance of the SW. Since SW performance is sensitive to a large number of external factors, this implies that SWs must be tested and evaluated under many conditions. And, since many of the factors that affect SW performance are probabilistic in nature (e.g. clutter or atmospheric conditions), several trials may be required to accurately characterize the system for a given set of conditions. For these reasons, SWs can create requirements for a large amount of test data.

Because of their importance to SW performance, the test environment and scenario must be representative of realistic conditions. This can present resource



Smart weapons can create large test matrices

problems because the desired environment or test targets may not be readily available. Also, it is critical that the tester properly characterize and record the important environmental

parameters during the test. Sometimes this can be tough to do because of the nature of the parameters to be characterized.

Second, SWs involve a number of complex subsystems that must work together to make decisions and autonomously engage a target. This may require that these subsystems be extensively tested individually to fully characterize the various subsystems' performance.

SW performance is dependent on many complex subsystems (e.g. seeker/sensor, signal processing, guidance and control, warhead and fuze). Without extensive and complex testing procedures, it may be hard to determine which subsystem may have contributed to a performance anomaly. Of particular importance are the seeker/sensor and the associated signal processing subsystems that are critical to making autonomous decisions concerning target engagement. This tends to stress testing of the sensor and signal processing subsystems, with a heavy reliance on captive flight tests (CFTs), drop tests, and tower tests.

Third, some types of SWs are many-on-many systems (many submunitions engaging many targets). This can require unique and extensive instrumentation that is capable of collecting the appropriate test data on many submunitions simultaneously engaging many targets.

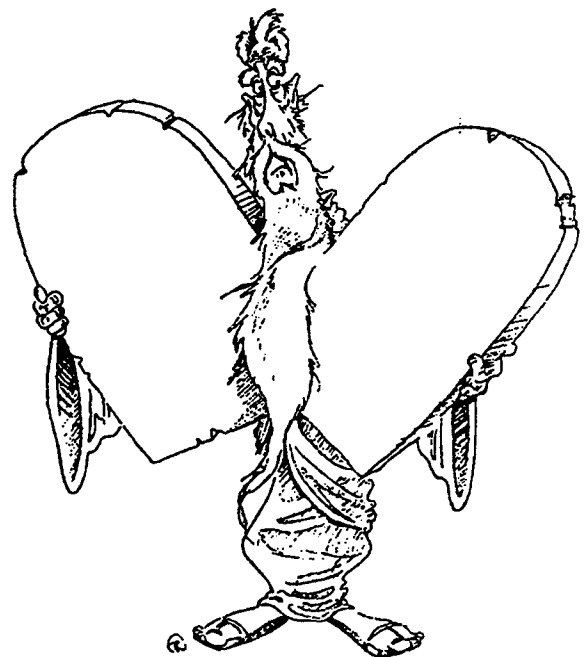
Testing resources have become a major issue for SW testing. The testing of many-on-many weapons stresses test resources and creates unique and complex test conditions. They may require uncommon test resources such as unusual test range

facilities or instrumentation. Furthermore, most SW systems and subsystems are relatively expensive. As unit costs increase it becomes prohibitively expensive to fire numerous test rounds. Alternative test strategies need to be developed. The same holds true for SW target sets. Employing and/or destroying these articles during a test can become an expensive proposition. This is an especially tough problem given the current tight fiscal environment.

These SW testing issues can create unique challenges for the tester. This guide discusses these issues and provides some suggestions on how to address them. This document also presents a number of principles related to SW testing. These principles summarize the issues and ideas of experienced SW testers. They are not in any particular priority; however, they are listed somewhat in chronological order in that the first six deal primarily with test planning and the last three deal predominately with test execution.

Principles for Successful SW Testing:

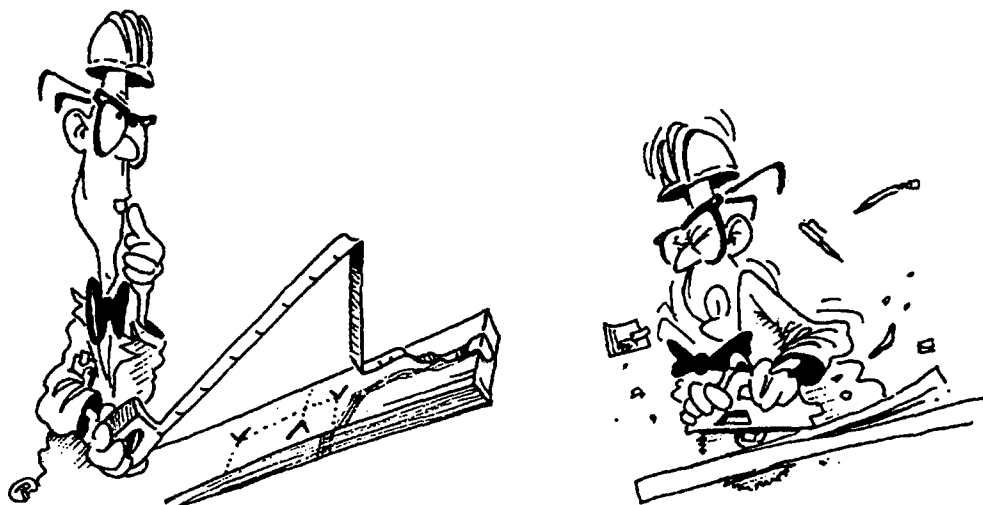
- ***Plan, plan, and plan again***
- ***Beware the long lead item***
- ***Validate your targets***
- ***Get your countermeasures blessed***
- ***Integrate testing and simulation***
- ***Work with your operational tester***
- ***Maintain strong test controls***
- ***Work with your data analyst***
- ***Collect good ground truth data***



Many of these ideas can be associated with the concept of concurrent engineering--a team approach to test planning and implementation. Concurrent test and evaluation essentially advocates full and open communication between all the players. It encourages the early involvement in the Test Integration Working Group (TIWG) and in the development of the test and evaluation (T&E) strategy and Test and Evaluation Master Plan (TEMP) by all participants.

2.1 Plan, Plan, and Plan Again

"Measure twice and cut once" is an old carpenter's expression. The same



adage applies to SW testing. SW testing is an expensive and complicated endeavor. Detailed and early test planning and coordination at all levels (TEMP, individual testing, etc.) can help make the testing run more efficiently and smoothly. Early coordination among all the relevant players is critical.

The test support community must be leaning forward in their foxholes to coordinate with the SW developers to develop, procure, and certify the specialized testing resources (primarily instrumentation and targets) that will be needed. These types of items can take a long time to develop and validate, and may even have significant technical, schedule, and budgetary risk associated with them. The earlier these needs are addressed the better. Furthermore, bringing the test support community into the process early may also ameliorate some of the data requirements. For example, when an analyst is not completely sure about what specific data will be needed, there is sometimes a tendency to ask for the world. This is especially true when dealing with target signature or clutter background data. The range people can

help point out some of the tradeoffs associated with collecting this data. Many of these types of instrumentation issues were addressed by Smart Munitions T&E Red and Blue Teams that were explicitly convened to address specific problems in defining and developing instrumentation for SWs. They examined SW test data requirements, instrumentation requirements, SW and instrumentation development schedules, cost

Some SW CM test planning experts that you can talk to for advice include:

Bob Bennett; Chicken Little: DSN: 872-8412; COMM: (904) 882-8412

Dan Hunt; VAL: DSN: 258-6204; COMM: (505) 678-6204

Chris White; SADARM PM: DSN: 880-3152; COMM: (201) 724-3152

Jack Bissinger; MICOM: DSN: 746-6144; COMM: (205) 876-6144

Dave Bundy; PM ITTS: DSN: 298-3634; (410) 278-3634

Gary Holloway; TECOM: DSN: 298-5270; (410) 278-5270

Brian Matkin; AMC SWMO: DSN: 788-8912; COMM: (205) 842-8912

drivers and budgetary issues. Their report [Reference 7] provides a good discussion of these issues.

With the declining defense budget and increasing test costs and complexity, it is imperative that the entire SW test community start sharing test resources. Early coordination of objectives can help this process. For instance, for a given test the DT tester may need to substitute instrumentation and telemetry equipment for the warhead, whereas the OT tester may want to have a warhead in the round to evaluate its lethality effects. Both these diverging objectives might be obliged by building some specialized rounds that can accommodate both instrumentation and warhead (as long

as they maintain operational form, fit, and function). However, these needs must be addressed early.

In order to have a successful test, there are numerous administrative, logistic, and technical support requirements that must be properly planned and coordinated in advance. Planning should begin as early as possible, although the exact time to initiate test planning and coordination will be dictated by the complexity of the test and the long lead items that need to be addressed.

There are two basic levels of test planning. The more general level of test planning outlines what tests should occur, when they should occur, and what their primary objectives should be. This higher level planning is primarily the function of the program manager (PM) and a variety of organizations interacting via the TIWG--the results of which are addressed in the Test and Evaluation Master Plan (TEMP), the technical Independent Evaluation Plan (IEP) and the developmental Test Design Plan (TDP). Each of these documents is summarized below in Figure 2-1 (See References 1, 15 and 18 for more information).

TEMP: The TEMP is the master document that outlines the T&E planned, completed, and contemplated on the system. It is prepared by the PM in coordination with the TIWG. The document identifies the required testing (both DT and OT), test personnel, test organization, materiel, facilities, troop support, logistic support, and funds for implementing the test programs.

IEP: The developmental IEP is prepared by the independent developmental evaluator (generally AMSAA) and coordinated among TIWG members. It addresses all aspects of the developmental evaluation responsibilities relative to the system. It details the actions that the independent developmental evaluator will take to evaluate the system. It states the technical characteristics, identifies

data sources, states the approach to the developmental independent evaluation, specifies the analytical plan, and identifies program constraints.

TDP: The developmental TDP is also prepared by the independent developmental evaluator and coordinated among TIWG members. It is responsive to the system's critical technical characteristics and includes a complete developmental test design, description of the required tests, the conditions under which the system is to be tested, and a statement of the test criteria and methodology. The developmental TDP includes plans for data collection/analysis and specifies data requirements.

The second, more detailed, type of test planning involves the specific arrangements necessary to carry out a particular test--the results of which are summarized in the Detailed Test Plan (DTP). The DTP is an internal document prepared by the organization conducting the test. This section deals with this more detailed level of test planning. However, it should be noted that any DTPs that are generated must implement the requirements of the TEMP, IEP, TDP, and other relevant documentation (see Figure 2-1) and will need to be closely coordinated with the TIWG and other organizations responsible for overall test planning. While this document focuses primarily on the performance testing of SW systems and subsystems in the field, it should be remembered that there are a number of ways to evaluate SW performance. These methods range from detailed laboratory component tests to full-up field tests. The common types of SW T&E methods are addressed in Figure 2-1.

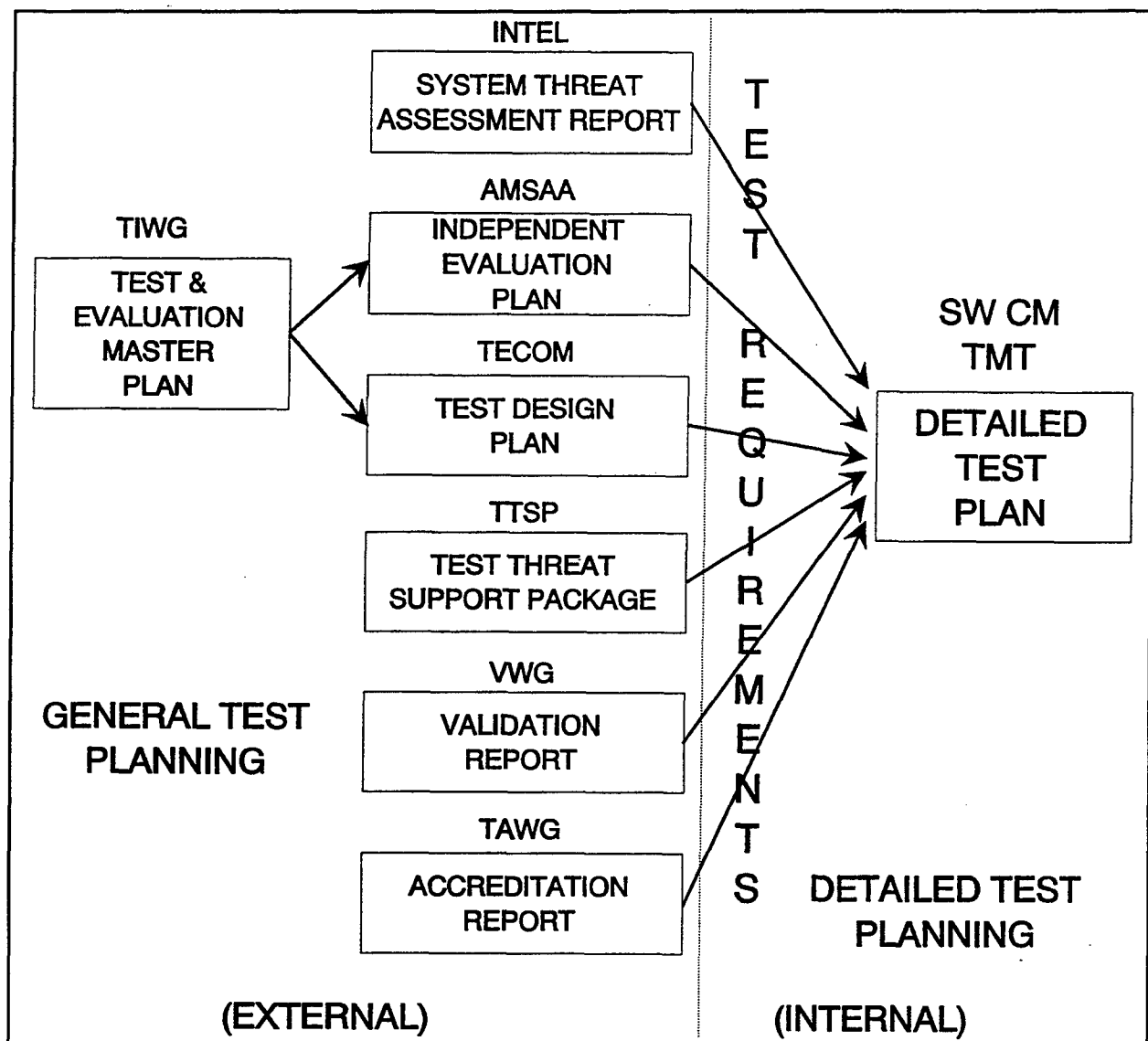


Figure 2-1 Detailed Test Plan

EXISTING DATA: It is important to realize that part of the required data may already be available. There are a number of databases and models available that might contain relevant information. These sources should be considered because some of the testing, and the associated costs, might be avoided.

References 20, 23, 24, and 25 provide good information on some of these existing data resources and their points of contact.

DIGITAL COMPUTER SIMULATIONS: An excellent method for obtaining a broad understanding of SW effectiveness is through digital computer simulations. This method is often the only cost-effective alternative for obtaining performance estimates in many-on-many, one-on-many and many-on-one operational scenarios. Although development of a SW model of sufficient detail to provide quantitative SW performance data can be costly and runtime prohibitive, qualitative data can indicate the sensitivities and trends which need to be addressed by a more quantitative testing method.

Typical computer simulation testing involves a Monte Carlo technique in which initial conditions of a simulated operational test are randomly selected. Performance characteristics of the SW are derived from the computed statistical parameters (mean, standard deviation, probability density, time correlations, etc.) of the resulting performance parameters (circular error probable [CEP], impact angles, impact velocity, lethality, etc.). Computer simulations usually offer the advantage of being able to supply statistical performance data based on large numbers of Monte Carlo runs in a wide variety of engagement scenarios.

Computer simulations are definitely limited in their ability to generate validated quantitative predictions of system performance in specific scenarios. This limitation is a result of the level of detail of the engineering models and signal environment models achievable in computer simulation; the difficulty in modeling system nonlinearities; and the lack of system model validation data. These difficulties can be partially overcome by employing hardware-in-loop (HWIL) simulations.

HWIL SIMULATIONS: In order to overcome the general inability of digital computer simulations to produce reliable SW performance data because of lack of detail in the system models and the large influence of system nonlinearities in SW performance, techniques have been developed to incorporate actual SW hardware and software in the simulation control loop. These HWIL simulations are generally conducted in special chambers in which target, background, and CM signals are generated at one end of the chamber and transmitted to the SW, located at the other end. The SW is usually mounted on a three-axis flight table used to simulate the angular motion of the SW relative to a reference line-of-sight. The simulation chambers are designed to minimize spurious signals resulting from reflections from the chamber walls or leakage from sources outside the chamber. The angular positions of the signal sources (target, CM, background) are typically controlled either by mechanical motion or by electrically switching to different signal emitters comprising a signal matrix array.

HWIL simulations, although normally restricted to one-on-one scenarios, are a primary source of quantitative SW performance data because of the representation of the SW and (some) active CMs by actual hardware. Other advantages of HWIL simulations include: the ability to evaluate real-time SW software in a controlled environment; the ability to vary target, background, and CM characteristics to test for SW sensitivities; and the ability to run Monte Carlo testing.

LABORATORY TESTS: SW materials, components, subsystems and techniques can be tested in a laboratory environment using laboratory grade instrumentation or chambers. These types of tests include component bench tests, environmental chambers, and special setups to determine the characteristics of SWs under controlled laboratory conditions.

TOWER TESTS: Tower signature measurements bridge the gap between the laboratory and field tests. They provide the basic set of target signature data for the SW designer or developer. Typically, signature measurements (with and without CMs) of targets of interest are made in the relevant spectral bands using calibrated high-resolution instrumentation. Data is usually gathered with the target mounted on a turntable arrangement and rotated through 360 degrees while data is taken at appropriate increments. The instrumentation platform is positioned vertically on the tower. The target/turntable is positioned horizontally from the tower; the target may be tilted to obtain the desired depression angles and ranges to the target. The cost and complexity of tower instrumentation testing is such that generally a coordinated requirements list from all the data users is factored into the data measurements requirements.

CAPTIVE FLIGHT TESTS: The primary objective of the captive flight test (CFT) is to determine the performance of the SW seekers and sensors engaging realistic targets and CMs in different environments. For a CFT, the sensors are mounted on a stabilized aerial platform in their operational configuration with on-board controls, instrumentation, computers, cameras, and recording equipment. Ideally the CFT is situated in an area where the terrain, environment, and weather closely match the anticipated operating arena. Sensor output data is recorded for the sensor package while it is flown over its target set at the correct altitude and approach angles enough times to establish a statistically valid number of data sets.

DROP TESTS: The purpose of a drop test is to test the sensor, signal processing, and lethality performance of a submunition in its terminal engagement phase. In the drop test, the submunition is suspended in air (or flown) over the target, and lowered at a controlled rate or dropped free-fall to simulate the actual descent conditions of the SW. The warhead can be fired at any elevation along its descent. The sensor's probability of detection (P_d) can

be tested at any elevation and repeated over and over. Test targets can be driven beneath the suspended sensor or, in some cases, the suspended sensor can be moved over a static target set.

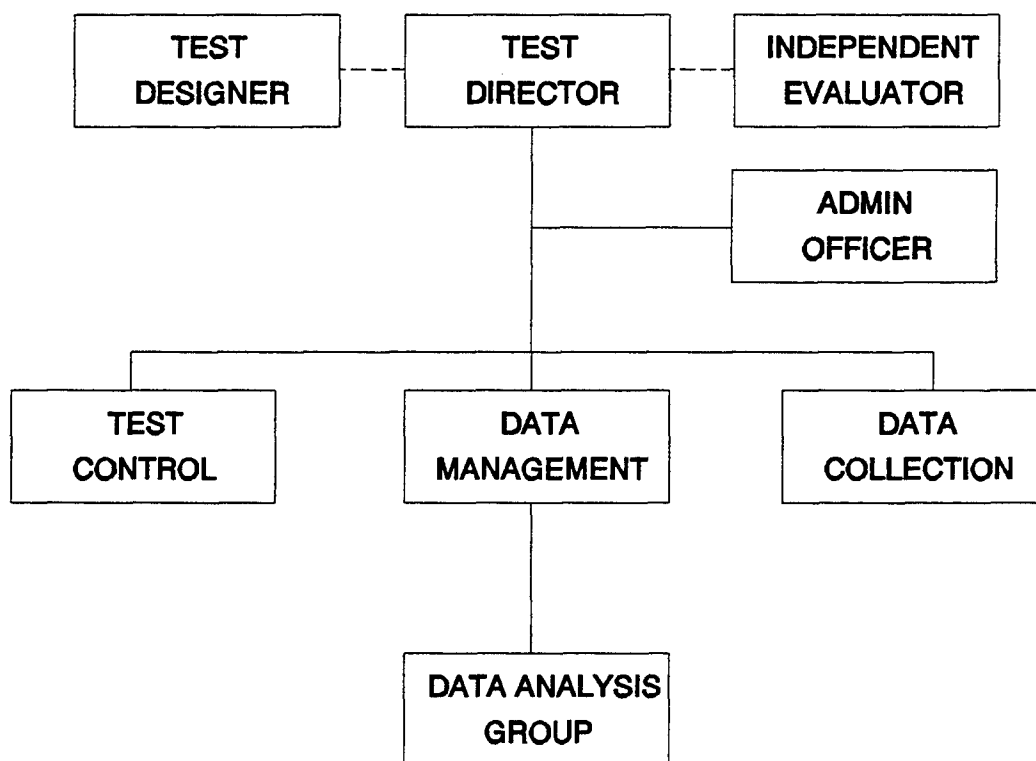
FULL UP TESTS: These are instrumented and full up SW tests involving the testing of fully integrated SW systems (or major subsystems) against targets and their CMs. These tests can involve either instrumented or tactical rounds. They are generally the most complex and expensive of the tests.

The basic activities involved in planning a typical SW CM test can be summarized as: Establishing the Test Planning Organization; Defining the Test Data Requirements and Test Matrix; Specifying and Arranging for Test Resources; and Generating and Coordinating the DTP. Each of these steps are discussed in Subsections 2.1.1 through 2.1.5.

2.1.1 Establish the Test Planning Organization

The first step in planning for a specific SW test is to establish the test planning organization. This test management team (TMT) can be a formal or informal group as dictated by testing needs. Its purpose is to manage and coordinate the programmatic, administrative, and logistical activities necessary to plan and implement the test and meet the test objectives. It also provides a convenient face-to-face forum for the resolution of test planning issues. A sample TMT organization for OT is diagrammed in Figure 2-2. Responsibilities of each of the TMT members are summarized below.

Test Director: Focal point for the planning and conduct of the test and responsible for the overall management of the test.



SOURCE: REF 27

Figure 2-2 Test Management Team Organization

Admin Support: Responsible for the administrative support such as security, office support, radios, etc.

Test Control: Coordinates with range personnel for support needed to implement and control scenarios such as targets, CMs, etc.

Data Management: Responsible for the collation, reduction, and reporting of test data. The sole release authority for quick-look and emerging data outside of the test directorate.

Data Collection: Responsible for the physical collection of the test data.

Data Analysis Group: Responsible for analyzing and interpreting the test data.

The TMT should conduct formally structured meetings with minutes, suspended action items, and reports to facilitate the efficient resolution of issues. The results of TMT planning must be closely coordinated with the appropriate agencies (generally the same ones that are members of the TIWG) to insure that the detailed test planning meets requirements. In addition to pulling together the test planning organization, the test director should initiate a project file. It should contain the type of information contained in Table 2-1.

- Checklists
- TECOM test directives with amendments
- Environmental documentation
- Requirements documents
- Independent evaluation plan
- Test and Evaluation Master Plan
- Applicable military specifications
- Contractor data
- Test plans (DTP, TDP)
- Threat documentation
- Safety documentation
- Security classification guide for End Item and Test Site
- Test incident reports
- All related correspondence and records such as:
 - Memorandums
 - Records of phone conversation
 - Memos for record
 - Minutes of meetings
 - Shipping documents - Trip reports
- Instructions provided to supporting elements
- Cost estimates
- Laboratory reports
- Reports from support elements
- Equipment logs
- Raw data
- Project log

2.1.2 Develop Test Data Requirements

The detailed test objectives will be designed to evaluate the technical and operational requirements of the SW system. The general system requirements are described in the Operational Requirements Document (ORD), Mission Need Statement (MNS), and other program documents. DT is conducted to determine if the hardware and software meet the system specifications. More detailed information related to system test objectives are provided in the system specification, TEMP, TDP and IEP. These test objectives must be translated into technical test data requirements and summarized in a test matrix. An example of a CFT test matrix is provided in Table 2-2.

Table 2-2 Example Test Matrix

MISSION	TARGET ARRAY(s)	STATIC ORIENTATION	TARGET COUNTERMEASURE COMBINATION				
			51	52	57	58	02
1	MMW1, 2, 3, 5	0°/180°	CM1	CM2			CM1
2	MMW1, 2, 3, 5	0°/180°	CM1	CM2		CM3	CM1
3	MMW1, 2, 3, 5	0°/180°	CM1		CM2	CM3	CM1
4	MMW1, 2, 3, 5	0°/180°		CM1	CM2	CM3	
5	MMW1, 2, 3, 5	0°/180°	CM3	CM1	CM2		
6	MMW1, 2, 3, 5	0°/180°	CM3	CM1		CM3	

SOURCE: REF 10

In planning for the collection of the required SW test data, it is important to consider that some of the data needed may already be available from other sources such as databases, models, previous tests, etc. This should be investigated because these other data sources may ameliorate the need for some of the testing (and the attendant costs).

In addition to the performance test data, there are several ancillary data requirements that must also be considered. An important one is ground truth data which characterizes and records the conditions under which the test was conducted. While the specific type of ground truth data that is required will differ based on the type of SW and the test objectives, there is some ground truth data that is generally common to most SW tests (See Table 2-3).

Other supplemental data requirements include quick-look analysis data and the test data needed to support simulations. It is especially important to work closely with the simulation and analysis personnel when defining these data requirements. The

analysts know best what performance and ground truth data they need in what format. The testers can work with them to insure that the test matrix is practical given realistic testing constraints.

Table 2-3 Typical Ground Truth Data

GROUND TRUTH DATA	
o	TARGET VEHICLE & CM POSITIONS/ORIENTATIONS
-	FLIR, PHOTOGRAPHIC & VIDEO RECORDS OF CM VEHICLES
-	RANGE INSTRUMENTATION POSITION MEASUREMENTS
-	POSITION OF IMAGING RADIOMETER
-	SENSOR POSITION & LINE-OF-SIGHT(LOS)
-	TIME TAGGED VIDEO CO-BORESIGHTED TO SENSOR LOS
-	SURVEYED TARGET LOCATIONS
-	TARGET STATES AND TEMPERATURES
o	ENVIRONMENT
-	BACKGROUND DESCRIPTION
-	RELEVANT BACKGROUND CLUTTER
-	GROUND TEMPERATURE
-	GROUND MOISTURE/CONDITIONS
o	METEOROLOGICAL
-	WEATHER DESCRIPTION
-	AIR TEMPERATURE
-	RELATIVE HUMIDITY
-	BAROMETRIC PRESSURE
-	WIND SPEED
-	WIND DIRECTION
-	PRECIPITATION
-	VISIBILITY
-	SUN ANGLE
-	SOLAR LOADING

2.1.3 Define Test Conditions

In addition to developing the test data requirements, the test planner must also define the test conditions. The test conditions to consider include the targets of interest, the CMs, the environment, and the scenario. Each of these test conditions must be specified so that test resource needs can be assessed and coordinated.

The conditions of the target and their attendant CMs must also be specified. The tester must consider such things as the type of targets, their relative placement and orientation, their operating states, their configuration, and their operational mode. Table 2-4 outlines the typical target test conditions that should be considered. Figure 2-3 outlines most of the types of CMs that should be considered in a SW test and Table 2-5 lists typical CM technical parameters. In developing the different target conditions, it is important to remember that a clean (uncountermeasured) target should be considered for inclusion in the target array to provide a baseline measurement condition.

Smart weapons may be strongly impacted by the environment in which they operate. For this reason, the selection of the appropriate environmental conditions is critical to SW testing. Examples of conditions that

Table 2-4 Target Conditions

TARGET TEST CONDITIONS
o HATCH OPEN/CLOSED
o HOT/COLD
o RECENTLY EXERCISED
o IDLING OR OFF
o MOVING OR STATIONARY
o BARREL ELEV/TURRET POSN
o RECENTLY FIRED OR NOT
o TACTICAL POSTURE
- DEFILADE
- STORES
- SPENT SHELL CASINGS

Table 2-5 Common Countermeasure Technical Parameters

SIGNATURE ALTERATION	DECOYS	OBSCURANTS	JAMMERS AND DEW
- o SUPPRESSION - MATERIAL - THICKNESS OF APPLICATION - MAP OF VEHICLE SURFACES COVERED - PERCENTAGE OF VEHICLE SURFACE COVERED - DECREASE IN AVERAGE RCS - DECREASE IN RCSs OF INDIVIDUAL SCATTERING CENTERS - DECREASE IN Δt - SUPPRESSED TEMP-ERATURE PROFILE MAP - o MODIFICATION - POSITION AND TYPES OF STORES - POSITION AND GEOMETRY OF GRIDS - POSITION, STRUCTURE, GEOMETRY OF IR KITS - INSTRUMENTATION MEASUREMENTS OF MODIFIED VEHICLE SIGNATURE - o AUGMENTATION - PHYSICAL SIZE OF AUGMENTING DEVICE - POSITION OF AUGMENTING DEVICE(S) RELATIVE TO VEHICLE - RCS OF RCR - HOT PLATE TEMPERATURE	- o PHYSICAL DIMENSIONS OF DECOY DEVICE - o POSITION OF DECOYS WITHIN TARGET ARRAY - o RCS OF RCR - o TEMPERATURES OF HEATED OBJECTS - o TEMPERATURE PROFILE AND SPECTRAL IRRADIANCE OF FLARES - o MATERIALS AND STRUCTURE OF MOCK-UPS	- o MASS EXTINCTION COEFFICIENT (α) OF OBSCURANT MATERIAL EMPLOYED - o INSTRUMENTATION MEASUREMENTS OF CONCENTRATION PATHLENGTH (CL) VERSUS TIME - o TIME HISTORY OF DEVELOPMENT OF OBSCURANT CLOUD IN RELATION TO TARGET ARRAY	- o JAMMERS AND HPM DEW - TRANSMITTER POWER DELIVERED TO ANTENNA FEED - ANTENNA GAIN AND 3dB BEAMWIDTH - ANTENNA PATTERN - ANTENNA SPATIAL ORIENTATION (TIME HISTORY IF VARIABLE) - CENTER FREQUENCY - MODULATING WAVE-FORM DESCRIPTION - AM OR FM - NOISE AMPLITUDE CHARACTERISTICS (MEAN, VARIANCE, PDF) - NOISE SPECTRAL CHARACTERISTICS (BANDWIDTH, PSD) - BLINK PERIOD AND DUTY CYCLE - SAMPLE CALIBRATED MEASUREMENTS OF TRANSMITTED JAMMER POWER DENSITY - o LASER DEW - ENERGY PER PULSE - PULSE WIDTH - PULSE PERIOD - BEAM DIVERGENCE

must be considered include the clutter background, atmospheric conditions, weather, and climate. More detail is provided in Table 2-6. Most of these environmental variables cannot be explicitly controlled. However, they can be influenced by the choice of when (date and time) and where (test site) to test.

The test scenario provides the backdrop for the script that details what the targets, CMs, and SWs will do and how they will interact during the test. The scenario script will dictate such things as when targets are static or moving, when they are in

defilade, what target formations will be used, when and how CMs are deployed, and how the SW will interact with the targets.

2.1.4 Specify and Arrange for Required Test Resources and Clearances

Defining and assembling the necessary test resources is one of the toughest, and most important, functions of the tester. There are a myriad of resources that must be allocated, within budget and schedule constraints, in order to set up a test. This can turn out to be a long list and it may be easy to forget something along the way. To help preclude this, a list is provided (Figure 2-4) that covers many of the test resources that might be needed and potential clearances to be considered. Working with a range project engineer can help make this process easier. See Table 2-7 for a list of major TECOM and common SW test sites.

One idea that was strongly suggested is to plan for a mechanism for procuring emergency incidentals during the test. For example, during one recent SW test, the test director was using flares inside of brass shells to simulate just-fired rounds. They quickly ran out of flares and ended up having to buy numerous flares at the local hardware store with their own funds. They were lucky that the quantity they needed was available and that they could afford to buy them. One way to allow for these types of incidental requirements may be to have a cash account specifically for this purpose. Another idea is to have test support contracts that allow for purchasing emergency incidentals during the test.

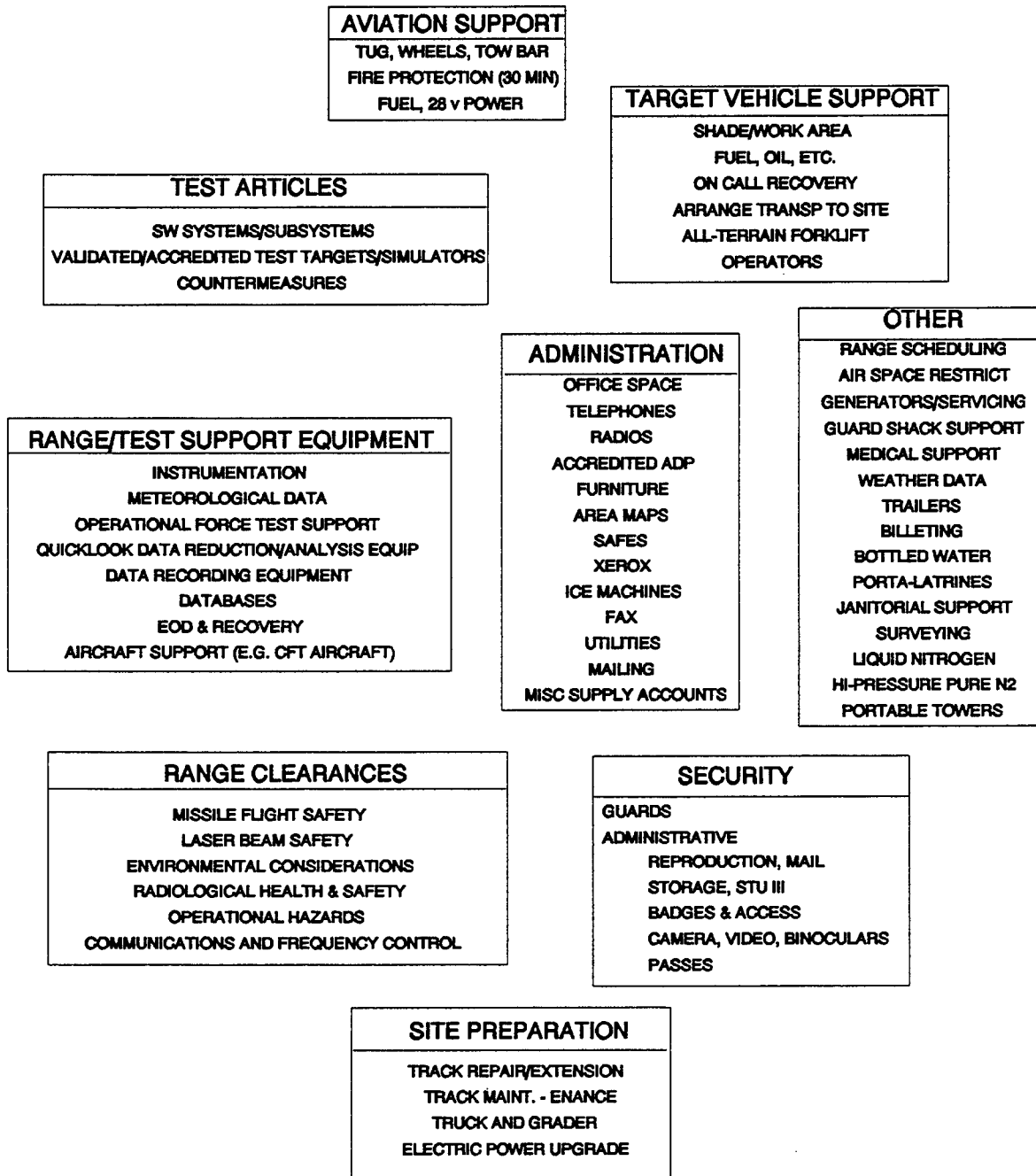


Figure 2-4 Test Resources and Clearances

Table 2-7 Potential SW Test Sites

TEST CENTER
COLD REGIONS TEST CENTER (CRTC); FORT GREELY, ALASKA
COMBAT SYSTEMS TEST ACTIVITY (CSTA); ABERDEEN PROVING GROUND, MARYLAND
JEFFERSON PROVING GROUND (JPG); MADISON, INDIANA
REDSTONE TECHNICAL TEST CENTER (RTTC); REDSTONE ARSENAL, ALABAMA
YUMA PROVING GROUND (YPG); YUMA, ARIZONA
WHITE SANDS MISSILE RANGE (WSMR); WHITE SANDS MISSILE RANGE, NEW MEXICO
ARMAMENT DEVELOPMENT AND TEST CENTER (ADTC); EGLIN AFB, FLORIDA
ARMAMENT RESEARCH DEVELOPMENT AND ENGINEERING CENTER (ARDEC); PICATINNY ARSENAL, NEW JERSEY
NAVAL WEAPONS CENTER (NWC); CHINA LAKE, CALIFORNIA
POKER FLATS RESEARCH RANGE (PFRR); FAIRBANKS, ALASKA
TONOPAH TEST RANGE (TTR); TONOPAH, NEVADA
UTAH TEST AND TRAINING RANGE (UTTR); EDWARDS AFB, CALIFORNIA
CAMP GRAYLING TEST RANGE; CAMP GRAYLING, MICHIGAN
FORT DRUM TEST SITE; FORT DRUM, NEW YORK

SOURCE: REF 11

2.1.5 Generate and Coordinate the Detailed Test Plan

The detailed test plan (DTP) is the specific blueprint for implementing the test. It provides explicit instructions for the conduct of the test. It specifies how the test data will be collected, reduced, analyzed, displayed, and used. There are three primary documents that provide information and guidance relevant to the development of the DTP: the TEMP, the IEP, and the TDP. The DTP is considered an internal document and there is no formal structure required by regulations. However, a suggested outline [Reference 9] is presented in Table 2-8 and other items to consider

Table 2-8 Suggested Detailed Test Plan Outline

SOURCE: REF 9

SECTION 1. INTRODUCTION

- 1.1 TEST OBJECTIVE**
- 1.2 TESTING AUTHORITY**
- 1.3 TEST CONCEPT**
- 1.4 SYSTEM DESCRIPTION**
- 1.5 UNIQUE TEST PERSONNEL REQTS**

SECTION 2. SUBTESTS

- 2.1 NAME OF SUBTEST**
 - 2.1.1 OBJECTIVES**
 - 2.1.2 CRITERIA**
 - 2.1.3 TEST PROCEDURES**
 - 2.1.4 DATA REQUIRED**
 - 2.1.5 DATA ANALYSIS/PROCEDURE**

SECTION 3. APPENDICES

- A. TEST CRITERIA**
- B. TEST SCHEDULE**
- C. INFORMAL COORDINATION**
- D. REFERENCES**
- E. ABBREVIATIONS**
- F. DISTRIBUTION LIST**

are provided in Table 2-9. A more detailed description of what type information the DTP should include is presented in Appendix B.

The DTP must be reviewed by the independent technical evaluator and should be coordinated with the TIWG to insure that it reflects the requirements of the TEMP, IEP, and TDP.

As the test date approaches, the TMT meetings should be held more frequently, and the number of people involved will grow. During the testing period, test conduct meetings should be held daily on-site to coordinate test matrix

changes/retests and quick-look analysis and discuss issues that come up during the test. The test director should make the determination as to what test organizations should be present at the meetings. The daily test conduct meetings will help insure that everybody is playing from the same sheet of music, so that changes to one part of the test don't create problems somewhere else.

The basic instructions for conducting the test will be found in the detailed daily test schedule/script (describes when mission activities will occur) and the mission summary/test matrices (describes what will occur). An example of a test matrix was provided in Table 2-2.

In addition to the mission test matrices for the collection of test data, missions should also be planned for system and instrumentation checkout. The purpose of these pilot tests is to wring out the data collection, reduction, and reporting methods, and exercise range support. Before any test missions occur the test site must be prepared: the site should be surveyed; targets, CMs, ground truth instrumentation and other test resources should be in place (based on surveyed locations) and ready; and flight/movement/engagement profiles should be fully mapped out and agreed upon.

Table 2-9 DTP Considerations

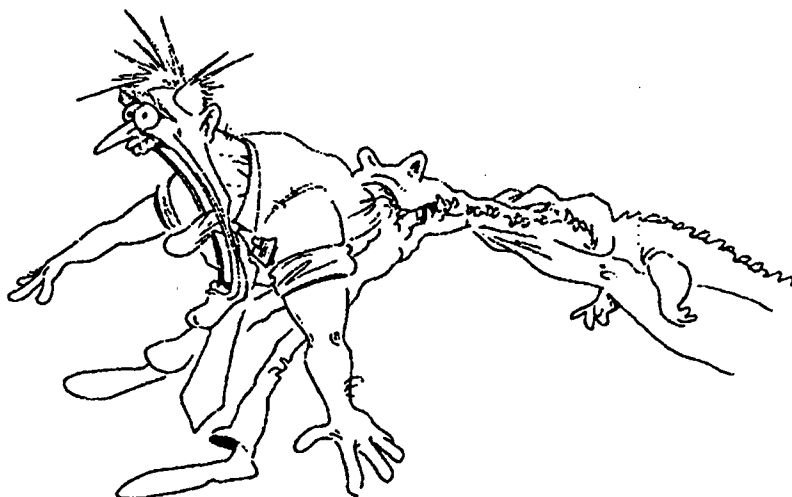
- PERSONNEL INVOLVED
- TEST SUPPORT RESPONSIBILITIES (WHO IS PROVIDING)
- TEST SITE LAYOUT
- SECURITY
- SAFETY AND OTHER CLEARANCES
- ROUTES/LOCATIONS
- MISSION LOG SHEETS
- TYPICAL DAILY MISSION SEQUENCE
- PREMISSION BRIEFING SEQUENCE
- MISSION TEST SEQUENCES
- TEST MATRIX
- COMMUNICATION LAYOUT
- VIDEO LAYOUT

DTP considerations in Table 2-9 address performance testing only. There are many other considerations such as natural and induced environmental, and electromagnetic and nuclear effects testing.

In summary, detailed and early test planning and coordination at all levels can help make the testing run more efficiently and smoothly.

2.2 Beware the Long Lead Item

Long lead items can cause unexpected problems and must be carefully managed. Some specific long lead items associated with SW testing include range clearances, test resources, and target validation.



There are a number of clearances that must be addressed prior to SW testing. The test range personnel should be able to define what clearances will be required. Many of the larger test ranges have staffs to support these documentation requirements (at a cost, of course). They include health, safety, and environmental clearances. For example, lasers, smoke, and any type of

AR 200-2 can provide information about environmental requirements

pyrotechnics can present a health and/or safety hazard and must be approved. Some SW systems pose sufficient hazards that they must contain a flight termination system to destroy them if they fly off course. Similarly, frequency allocations and electromagnetic interference

(EMI) must be considered. For instance, radio frequency (RF) jammers and chaff can affect local air traffic control and navigation. Radar systems can present a radiological health hazard. For tested articles, the responsibility for issuing a safety release belongs to the PM. For instrumentation, this is a range responsibility. Environmental clearances can be a very long lead item and become a genuine show stopper. For

example, the average time for environmental assessments at WSMR has been seven months; an environmental impact statement is more likely to take eighteen months [Reference 5]. See References 4 and 23 for more information about environmental requirements. Countermeasures such as smoke, fog oil, noise, chaff, jammers or foliage can impact the environment and must be addressed. For example, a typical field expedient CM involves applying foliage to the vehicle or target. Cutting vegetation for foliage can adversely affect the environment and people have gotten into trouble for this. This type of activity must also be suitably approved.

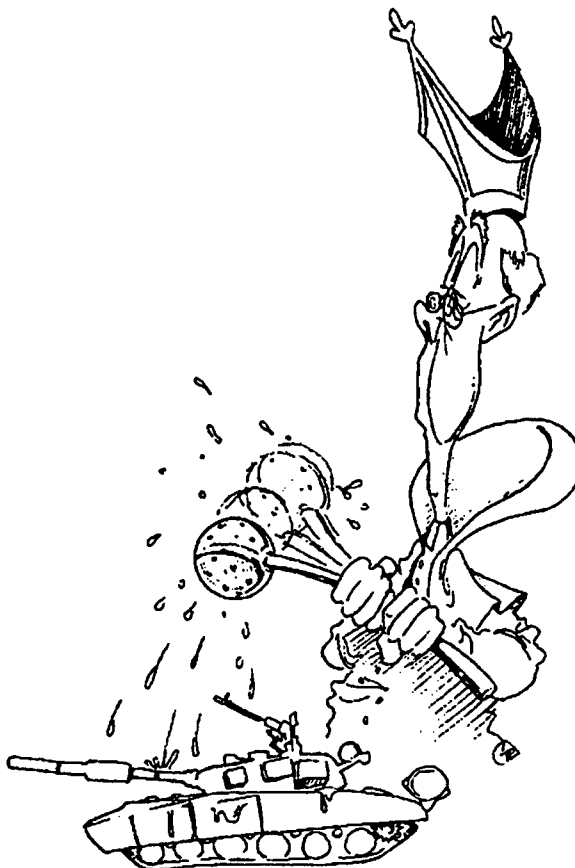
Environmental concerns can impact the test in other ways. For example, in one case the exhaust from a foreign vehicle created a light oil spot. During the test, range personnel were mopping up the oil as it accumulated on the ground. While this was the correct thing to do from an environmental perspective, removing the warm oil could bias the test by changing the signature perceived by the SW sensor. Another interesting problem that has come up involves historical sites. In some cases, testers have had to modify or move their testing so as not to disturb potential archeological sites. Some testers also ran into problems with endangered species that required them to move their test site. Any modification or preparation of the test site that involves facility engineers can involve very long lead times. Almost all the experts recommend that anyone needing extensive range clearances, especially when dealing with environmental issues, should definitely try to test in areas where these types of clearances have been previously granted. This can save the tester a lot of time and effort in preparing the necessary studies and paperwork.

Another long lead item to consider are the specialized test resources that may need to be procured or developed. This includes specialized CMs such as jammers or decoys. Even relatively common CM items such as nets may become long lead items, because it can sometimes take a long time to order and receive them--and invariably the first order will be of the wrong type or arrive late. Of special concern to SW testers is the specialized instrumentation that may be required to support the testing. Some SW test programs are having tough problems because the unique

instrumentation required to support them is extremely expensive and must be developed. And unfortunately, their testing schedule is dependent on the instrumentation being available on time. Another potential long lead item is the target set that the SW will be tested against. Many times, real targets are not available in sufficient numbers to adequately support the test. In cases like this, target simulators (fake targets that are fabricated to mimic the signatures and other important characteristics of a target) must be developed, or a target surrogate must be found. Target surrogates are similar targets that are sometimes modified and used as a substitute for the real target. Since target characteristics can strongly impact the performance of SWs, it is important that these target characteristics be correct. For this reason, SW test targets must be validated and accredited by the appropriate authorities (This process is discussed in the next subsection.). The target validation and accreditation process, as well as the target simulator development process, can become long lead items that must be considered and prudently managed.

2.3 Validate Your Targets

To be suitable for SW testing, threat targets must be validated and accredited. This authentication process is required because the characteristics of a test target can strongly impact the performance of a SW. Validation may be required for real targets as well as for target simulators and surrogates. The rationale for requiring real targets to be validated is that even actual targets may not be an accurate representation of the typical target that the SW may be expected to encounter. For example, if the real target is poorly tuned, it may run hotter than a typical target. This might bias the test by making it easier for an infrared seeker to detect the target.



The development of accurate target simulators can be a tricky process. This is because signatures can be complex and hard to imitate. This is especially true when dealing with multiple spectral bands, if moving targets are needed, or if ballistic fidelity is required. Furthermore, the application of CMs to a simulator can magnify any differences between its signature and the real target. For example, in one case a simulator was developed that had a signature slightly less intense than the real target. However, when the simulator was placed under a net, which reduced its signature, this small signature disparity between the simulator and target was magnified and it made the difference between detecting and missing the target. In another case, when

both a target and simulator were placed under a net, the SW performance against the target was better than against the simulator. As it turned out, the exhaust on the real target was configured in such a way that it heated the ground outside the net. The SW was occasionally detecting this heated ground and firing at the ground. Some of the shots hit the target. This improved its overall performance. The simulator did not produce exhaust emissions. Instead it was heated with electric coils and did not warm the surrounding soil. This reduced the SW's performance against the simulator.

Target simulator development can be an expensive and time consuming activity. The Project Manager for Instrumentation, Targets, and Threat Simulators (PM ITTS) can provide help in procuring or developing targets. PM ITTS has different responsibilities, depending upon whether one is interested in a target simulator or a real target. PM ITTS is responsible for developing the technical specifications and building a first prototype target simulator and getting it validated. The SW PM can then build, with his own funds, as many copies of this prototype as are needed for testing. Unfortunately, the development of the first validated target simulator prototypes is constrained by PM ITTS budgetary restrictions. For this reason, it may be necessary to pay for the prototype development also. PM ITTS also has a number of actual (real) foreign targets (T72, 2S1, 2S3, BMP1, BMP2, BTR70, ZSU-23/4, ACRV, MTLB and wheeled vehicles) that can be borrowed or rented from their library (and returned in the same shape). And, if PM ITTS does not have the target needed, they may be able to procure it from one of their many sources. They also have a pretty good idea of who is using what targets, and may be able to help borrow one from someone else. For example, targets are also available from such organizations as the Chicken Little project office, MICOM, and TECOM. Another issue

**PM ITTS can help with targets and simulators. Call Dave Bundy at
DSN: 298-3634; or
COMM: (410) 278-3634.**

that can complicate testing is the fact that some real foreign targets are classified (although this seems to be easing with the dissolution of the Warsaw Pact). Classified targets can impose security administrative burdens on the tester in terms of limiting access to cleared individuals and restricting test windows (e.g. testing is allowed only when foreign satellites are not overhead).

The target validation process falls under the purview of a Validation Working Group (VWG) which authors the Target Validation Report. Target accreditation is the responsibility of the Target Accreditation Working Group (TAWG) which authors the Target Accreditation Report. The TAWG is subordinate to the TIWG. Both working groups are made up of technical and user representatives from a number of developer and user agencies to include: TECOM, DA DCSINT Threat Integration Staff Officer (TISO), AMSAA, PM ITTS, MSIC, FSTC, TRADOC, ARL, RD&E Centers, and others as required. More detail is available in Appendix A which contains the DAMO-FDZ memorandum "U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets." This memorandum explains the target validation and accreditation process. It should be noted that this process is undergoing review and may be changed.

The VWG validation of a target is a generic analysis that looks at the differences between a target and its simulator. It is generally conducted only once. However, if the threat changes or if the simulator changes (such as being shot and repaired numerous times), re-validation may be required. After a target is validated, it must be accredited for use by a specific system. Whereas validation is usually conducted once, accreditation can be done many times, once for each system that tests against the target. Unfortunately, the validation looks primarily at generic differences (e.g. appearance, drive train, etc.), rather than specific differences relevant to a particular weapon system (e.g. signatures at a unique spectral band and aspect angle). This means that the validation report might not completely satisfy requirements for a specific SW system. This implies that the detailed analyses specific to that weapon system may need to be conducted during the accreditation

process. Fortunately, the intelligence community tries to anticipate which systems will require the information, and conducts their target validation accordingly.

The TAWG uses the Validation Report as one of its inputs to generate its Target Accreditation Report which is provided to the chairman of the TIWG (usually the SW PM). The TIWG chairman approves or disapproves the TAWG's accreditation recommendations.

In summary, threat targets must be validated and accredited in order to be suitable for SW testing. This can be a lengthy and complicated process involving a lot of different players and must be addressed early.

2.4 Get Your Countermeasures Blessed

Countermeasure testing is both an art and a science. While CM testing is a technical discipline, it can also be a highly subjective process without firm rules. Consequently, it can be a point of contention for many people. This is especially true when it comes to deciding the detailed characteristics of the CMs to test and how to apply them to the target. For example, there have been many arguments over how foliage should be used as a field expedient CM. In some cases,

**Confirm your assessments
(CYA)**



CM testers have been criticized after the fact about how green the foliage was, how long ago it was cut, how much was applied, and how tightly it was attached to the target. Occasionally, tests had to be redone.

An important motto for CM testing is "confirm your assessments (CYA)." The best way to accomplish this is to work

closely with the intelligence community to get the CMs blessed. This is especially important today with the threat in a constant state of flux.

General information and requirements concerning CMs that need to be tested are contained in the System Threat Assessment Report (STAR), the Threat Test Support Plan (TTSP), the Test and Evaluation Master Plan (TEMP), the Operational Requirements Document (ORD) Survivability Annex, and other documented sources of validated threat information for the SW of interest. When reviewing these documents, they should be checked to make sure they are consistent in their threat and CM information--sometimes they do not match. Unfortunately, these threat documents generally provide only high level requirements information and do not provide direct specific CM guidance for testing. The Vulnerability Assessment Laboratory (VAL) and other relevant intelligence sources such as the local Foreign Intelligence Office (FIO),

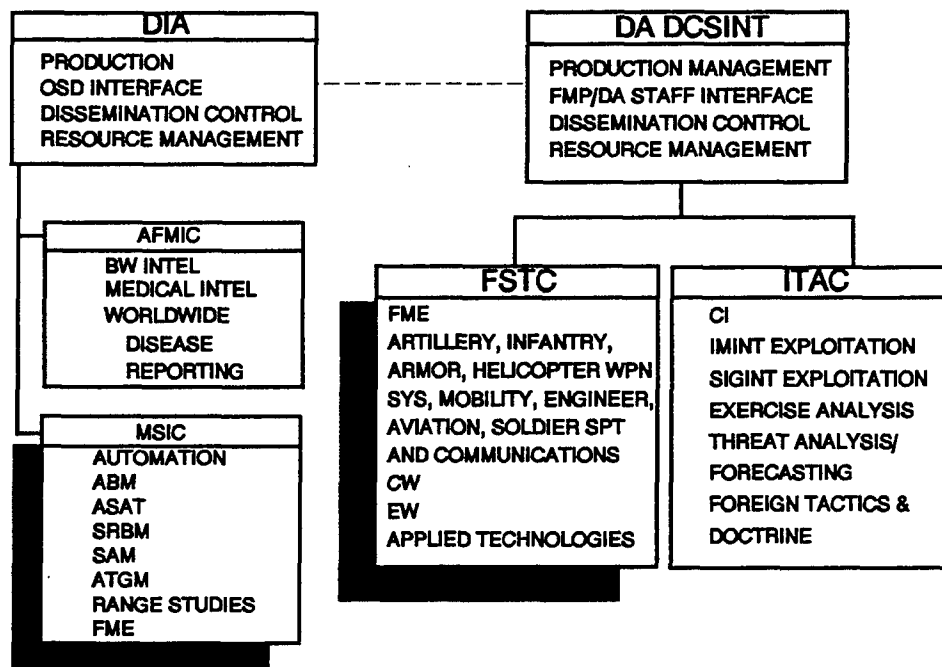


Figure 2-5 Intelligence Agencies

the Foreign Science and Technology Center (FSTC) and the Missile Space Intelligence Center (MSIC) can provide more detailed guidance and interpretation. Another good source is the weapon system Threat Integration Staff Officer (TISO). It should be noted that these production centers recently underwent a reorganization (See Figure 2-5). Usually, the best approach to determining the specific characteristics of the CMs to be used during a test is to pull together an ad hoc CM working group to address these concerns. The working group should contain representatives from the user, FSTC, VAL, FIO, and other appropriate agencies. This ad hoc CM working group should be subordinate to the TMT, and may include many of the same TMT members.

Testers need to be proactive with the intelligence community, because the formal process is not designed to provide precise details about which CMs should be used in a particular test, as well as how. The tester needs to ask specific questions and get enough detail to reproduce the CMs in the field. One very good suggestion is to invite the intelligence analyst to the test. Send travel money if required. The analyst can get an idea of the practical concerns related to applying CMs in the field, and the tester may learn some new threat information. Both parties may come away smarter. In any case, the intelligence analyst will be much more likely to come to the tester's defense if he helped put the CMs on the target. Another suggestion is to get actively involved in the TAWG, TIWG, or other test working groups to get the detailed CM plans documented in their reports. These groups generally include a number of different representatives from the intelligence community and other agencies who may provide fresh perspectives on the CM ideas.

**Invite the Intelligence Analyst to
Your CM test.**

2.5 Integrate Testing and Simulation

As was discussed earlier, SW testing can generate large test matrices that can strain testing capabilities. Because SWs are affected by the environment in which they operate, it is generally not feasible to test under all the relevant conditions that may impact system performance.



There are two basic categories of testing that are relevant to this discussion: developmental testing (DT) and operational testing (OT). Each has a different objective. The basic purpose of DT is to provide test data to establish and confirm performance boundaries and to ensure that it meets performance specifications. This data is used to design and develop the system. The testing is not necessarily conducted in accordance with any doctrinal configuration; extensive instrumentation may be present; and the testing is technically oriented. The principal goal of operational testing is to provide operational performance information on the system functioning as it would in the field. Operational tests are generally conducted in their field configuration with actual troops manning the system. Simulations are used to evaluate boundary performance, fill out

the test matrix, and conduct sensitivity analyses. They can also be used to estimate system performance data for conditions under which it may not be possible to test.

The generally accepted approach to system evaluation used to be that simulations and developmental testing were conducted to generate the data needed to develop the system. Because this data was used primarily for development, these tests were designed to stress the performance of the system at its potential weak points. Operational testing, on the other hand, was conducted as essentially a pass/fail test after the system was developed (using pre-production prototypes or production items). DT and OT were generally conducted independently of each other. However, because of testing and funding constraints, this previous approach has been evolving to a new strategy where DT, OT, and simulation results are all used to form an integrated picture of SW performance (See Figure 2-6).

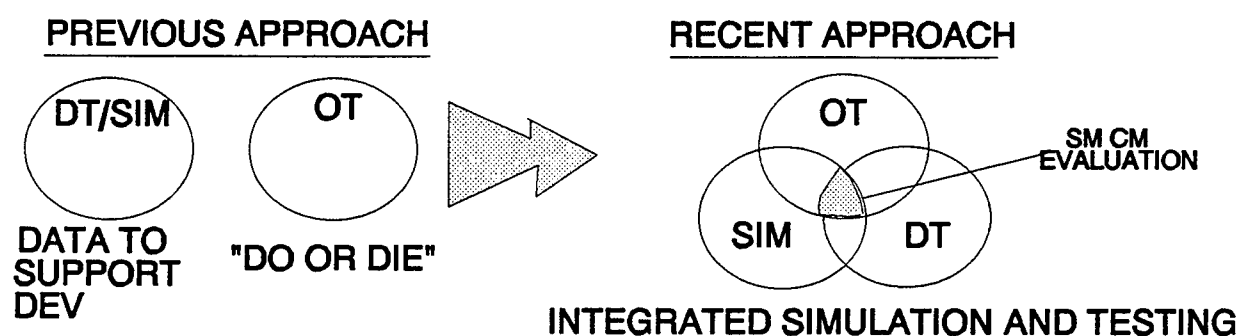


Figure 2-6 Approach to DT and OT

This is especially true as simulation techniques and computational hardware become more sophisticated and weapon systems become more complicated and expensive. For example, the NASA shuttle never had a full-up flight test before its maiden flight with humans aboard. It was too expensive to test. Instead the results of numerous simulations and subsystem tests were used to verify its performance. Conversely, the TOW missile, a relatively inexpensive and simple system, underwent

numerous full-up flight tests prior to production. Full-up testing was used because it provided the most reliable results and it was cost effective to do.



than simulation, testing results usually have more credibility than simulation data. Simulations, on the other hand, are much more flexible and cost effective.

Testing should be used to provide point data for critical performance questions. "When in doubt, test" is a good rule of thumb. Tests should be planned so as to also collect data that will support the validation of supporting

**Have a good
simulation
validation
plan.**

simulations. It is also a good idea to try and "piggyback" off tests to collect required input simulation data such as background or target signatures.

In integrating simulation and testing, it is important that the test planner use them together in such a way as to capitalize on their strengths and reinforce each other. While testing is generally much more costly

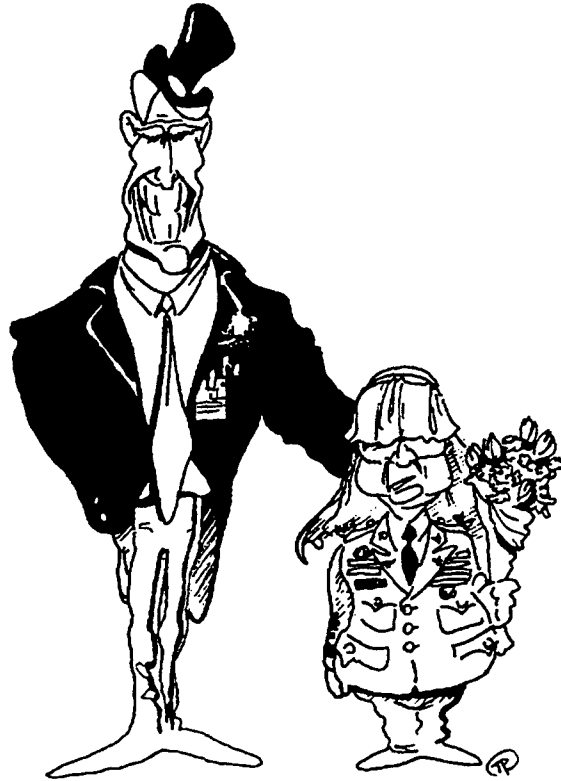


Simulations (both digital and HWIL) can be used to extrapolate test data and to support test planning. Because of their flexibility, simulations can provide SW performance estimates for conditions under which it may be impractical to test. And, when planning for a test, simulations can provide an idea of what kind of performance to expect during the test. This type of data can help identify system performance boundaries to design the test, and provide a baseline sense check to help identify any anomalies that may occur during testing. It is important to note that one must be careful about how simulations are used. Validation of the model is critical to its credibility. Simulation validation should be planned and implemented as an integral part of the simulation development process (rather than after the fact). Simulations can give a false sense of security to the user. First, the level and detail of data necessary to properly run the simulation may not be available. Second, it must be remembered that many complex or random events can occur, especially with CM effects or when there is a man-in-the-loop, that cannot be adequately predicted or modeled in a simulation. In these types of situations, hardware-in-the-loop (HWIL) simulations (which are kind of a hybrid between digital computer simulations and testing) might provide more accurate answers because HWIL simulations use actual SW hardware that may replicate any unexpected hardware operating conditions.

2.6 Work With Your Operational Tester

In the past, the operational tester started testing after the design was frozen and the system was nearing production (using pre-production prototypes or production items). However, as systems become more complex, test requirements increase, and test resources become harder to get, it is inevitable that DT and OT will start concurrently. This approach can create several advantages, disadvantages, and issues that must be addressed by the SW tester.

The obvious advantage to combined DT and OT is in conserving test resources. There are also several other benefits. When the operational tester participates in the developmental testing, he is more apt to understand how the system functions and the subtleties involved in why it performs the way it does. This understanding may help the operational tester conduct his tests more efficiently. Or he may be able to accept DT data and forego some OT altogether. Also, the operational tester may be able to provide suggestions to the developer that will make the system better for the troops in the field.



Concurrent DT and OT is becoming more commonplace.

There are also some disadvantages to conducting

concurrent DT and OT. Most importantly, the DT and OT objectives may conflict (DT usually wants a lot of data under controlled conditions, whereas OT usually wants limited data under uncontrolled conditions.). For example, an OT objective may be to test the ability of the SW gunner to find a target in the presence of smoke. The DT goal may be to test the ability of the SW to operate through a specific level of smoke. While these two objectives seem compatible, they may actually conflict. For instance, in order to measure the level of smoke in the area, the CM tester will want to position instrumentation near the target so that it can accurately measure the smoke conditions. This might bias the OT because the gunner could easily locate the target by looking for the instrumentation vans. This type of problem has actually occurred. Another potential problem that may occur is that operational testers may start "evaluating" the system while it is in early development, before the engineering design has been fully completed. They may start forming opinions about the system before it is ready for strong scrutiny. This problem may intensify as the military budget tightens and the budget people look for ways to save money. The SW PM may spend a lot of his time defending DT data that was collected for development purposes and was not meant to be interpreted or used as a pass/fail test.

Essentially, the process of accommodating both DT and OT objectives in the same test is one of negotiation and compromise. If the operational testers will be piggybacking on a developmental test, then they should be involved in all relevant aspects of the planning. Their needs should be obliged when feasible, but not at the expense of DT objectives. And DT test data should be used by OT evaluators only with the understanding as to the meaning, purpose, and appropriate uses of the data.

2.7 Maintain Strong Test Controls



During testing, it is important to maintain a strong grasp on what is happening. A lot of energy should be focused on planning and developing the SW test matrices and test plan. A well conceived and efficient test plan will help the test run more smoothly.

The test plan is the blueprint for the test and it is important to try to stick to the it. Any impromptu changes to the testing, if they are not fully reflected in the test plan, could hinder the test schedule or objectives. This said, it is also important to recognize that given the way things work, it will probably be necessary to make changes during the test. As unplanned requirements arise or as the testers learn from the testing, changes will be required. In any case, these changes to the test must be

carefully controlled. They must be fully deliberated and reflected in the test plan before they are implemented. A process must be in place to allow for quick and efficient modification and coordination of the test plan. This way everyone will be working off the same test plan. Otherwise, the test director can quickly lose control over what is happening in a complicated test. Many experts advise that the test director have at least daily coordination meetings during the test (before and/or after each test day or pre-mission briefing and post-mission debriefing) to coordinate test matrix changes and other issues. Everyone should be playing from the same sheet of music so that changes to one part of the test don't create problems somewhere else.

It is important to take copious notes during testing. Remember, someone has to use the test data that is being collected, and it is important that they understand the conditions under which the testing occurred. In addition to data logs and audio records, photographic, infrared, or video cameras are ideal for explaining what was done and what the conditions were during a test. All records should be appropriately time stamped. Invest the time and resources necessary to have an efficient quick-look analysis and database capability. Real-time results can be used to explain what is happening or answer questions during the test, such as a root cause analysis of an unexpected failure. Quick-look data can also provide a good means of checking the integrity of the data while it is being collected. This will help detect and fix problems and improve test procedures while everyone is still in the field. It is usually too late to fix bad data if a problem is discovered after the test is finished. However, it is important to guard against the indiscriminate release of quick-look data outside the immediate test cell. Much of this data may be incomplete or may not accurately reflect overall performance and might elicit premature conclusions.

2.8 Work With Your Data Analyst

It is important to foster good communications between the people taking the test data and those who will use it. Both the analysts and testers should work together to generate the test matrix. The analysts are the best ones to know what data they need and in what format. They can help ensure that the test matrix satisfies their needs--not only for SW performance data, but also for other data such as ground truth measurements. The testers can then apply a measure of practicality to the analysts' requests. Having the simulation and analysis people working closely with the tester also fosters the integrated approach to SW evaluation. As was discussed earlier, simulation data can be used to help plan the test, and testing should support simulation validation and data requirements. If possible, bring the simulation and analysis people to the field during testing. That way, they can observe for themselves the conditions under which the test was conducted. They will learn some of the problems that can crop up in trying to implement a test matrix and learn how to design more realistic test matrices in the future. And if test problems come up, they may also be able to help adjust the test matrix to work around the predicament. They can also provide help in reducing and analyzing the quick-look data during the test. It may even be advantageous to consider putting the analysts in charge of collecting the test data with the testers providing support.



2.9 Collect Good Ground Truth Data

Because SW systems can be strongly affected by their operating environment, it is important that the critical environmental parameters be recorded properly. Without the appropriate ground truth data, it may not be possible to properly analyze the test data results.



Good ground truth data can help interpret what occurred during a test. For example, in one case it was noted that every time it rained a particular SW's detection performance dropped. It was initially thought that this occurred because the rain cooled the target. However, because they had good ground truth data, the analysts were able to determine that instead, the rain warmed the background to make it more like the target.

Ground truth data should be collected at the same time, location, spectral band, and boresight of the system of interest. One mistake that is commonly made is to collect the ground truth data sometime before or after the test. Ground truth data collected under these conditions may not be valid because the relevant environmental conditions can change markedly over even a matter of minutes. For example, the shade from a cloud moving overhead may change the IR signature of a target and background enough to significantly affect the test results.

One good way to have calibrated data is to do side-by-side testing. That is, a clean (uncountermeasured) target is placed near countermeasured targets. In this

way the tester can be reasonably sure that the environmental conditions were approximately the same for all of the targets. In addition to dedicated ground truth instrumentation, it may also be possible to use the SW sensor itself to collect ground truth data by training it on referenced targets such as calibrated reflectors. The appropriateness of this method will strongly depend on the technical characteristics of the sensor and the objectives of the test.

Another important consideration when collecting ground truth is the effect that the CMs will have on the ground truth instrumentation. For example, flares designed to impede the operation of SW IR sensors may also negatively impact the operation of IR ground truth instrumentation. It doesn't make much sense to try and collect ground truth data with instrumentation that will be made inoperable by the CMs. Instead, the test must be designed to preclude these types of problems. One key point concerning ground truth data is that it should be made a part of the formal data requirements to ensure that it is properly collected along with the other test data.

3.0 SUMMARY

Smart weapon testing can present unique challenges to the tester. This guide discusses these issues and presents some testing principles that address them.

These principles include:

- Plan, plan, and plan again
- Beware the Long Lead Item
- Validate Your Targets
- Get Your Countermeasures Blessed
- Integrate Testing and Simulation
- Work With Your Operational Tester
- Maintain Firm Control During Testing
- Work With Your Data Analyst
- Collect Good Ground Truth Data

These principles of SW testing provide a good framework for implementing a SW test. In addition to these ideas, there are also a number of references and points of contact that can be accessed to provide guidance in planning, coordinating and implementing a SW test.

Appendix A

U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets

Reference. The information in this appendix was reproduced from the following source:

DAMO-FDZ Memo: U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets, HQDA, February 1991.



DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR OPERATIONS AND PLANS
WASHINGTON, DC



REPLY TO
ATTENTION OF

FEB 19 1991

DAMO-FDZ

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets

1. The enclosed Army Validation and Accreditation Plan for Threat Simulators and Targets, dated February 1991, is forwarded for implementation. This plan updates the previously published document by including procedures for operational validations which take place after target and threat simulator systems have been fielded. Target and Threat Simulator Validations and Accreditations are relatively new concepts. As we work with these plans we should expect to achieve additional improvements. Your cooperation in implementing and refining this plan is appreciated.
2. POC is Major Frank G. Atkins, DAMO-FDT, Autovon 225-3820.

Encl
as


JEROME H. GRANRUD
Major General, GS
Assistant Deputy Chief of Staff for
Operations and Plans, Force
Development

DISTRIBUTION:
DUSA-OR (SAUS-OR)
ASA(RDA) (SARD-ZR, SARD-RP, SARD-IP)
DESINT (DAMI-FIT)
DCSOPS (DAMO-TRS, DAMO-FDT)
DISC4 (SAIS-P)
DPA&E (DACS-DPM)
Army Intelligence Agency (AIA-IPD-FMB, AIAMS-ZA, AIFR)
Army Materiel Command (AMSTE-TD, AMSLC-VL-CB, AMXSY-A, AMCCE-TE-E)
Army Training & Doctrine Command (ATCD-EP)
Operational Test and Evaluation Command (CSTE-PO-I, CSTE-OT, CSTE-PO-T)
ASAFM (SAFM-CA-ZA)
Office of the Surgeon General (DASG-HCD)
Strategic Defense Command (CSSD-TE-T)
Information Systems Command (ASPL-A)
Test and Evaluation Management Agency (DACS-TE)
Program Manager ITTS (AMCPM-ITTS)
Army Missile Command (AMSMI-WS-T)

**U.S. ARMY
VALIDATION AND ACCREDITATION PLAN
FOR
THREAT SIMULATORS AND TARGETS**

FEBRUARY 1991

NOTICE

This plan supersedes the Validation Plan dated August 1990 issued by HQDA, DCSOPS.

TABLE OF CONTENTS

	PAGE
1. INTRODUCTION	1-1
a. Purpose	1-1
b. Authority	1-1
c. Scope	1-1
d. Validation/Accreditation Support to Materiel Development	1-1
e. Definitions	1-1
f. References	1-2
g. Publication	1-2
2. VALIDATION	2-1
a. General	2-1
b. Responsibilities	2-2
c. Validation Process	2-3
d. Validation Decision Points	2-3
e. Validation Working Group	2-4
3. ACCREDITATION	3-1
a. General	3-1
b. Responsibilities	3-2
c. Threat Accreditation Working Group (TAWG)	3-4
 List of Figures:	PAGE
1-1 Validation/Accreditation Support to Materiel Development	1-4
2-1 Threat Simulator/Target Life Cycle	2-1
2-2 Validation Working Group	2-7
2-3 Validation Event Cycle	2-8
3-1 Threat Accreditation Working Group	3-6
3-2 Threat Accreditation Event Cycle	3-7

Enclosures:

- 1 Abbreviations and Acronyms
- 2 Validation Report Format
- 3 Threat Accreditation Report Format
- 4 Definitions

1. INTRODUCTION

a. Purpose. This plan describes the Army Validation and Accreditation Program for Threat Simulators and Targets. In this plan, the concepts, processes, policies, and procedures employed in validation and accreditation are defined and prescribed. The roles and responsibilities of the Department of the Army agencies and organizations involved in validation and accreditation are identified and explained. These procedures implement Department of Defense guidance concerning threat simulators.

b. Authority. This plan is issued under the authority of AR 381-11, Threat Support to U.S. Army Force, Combat, and Materiel Development; and DoD 5000.3-M-6, Threat Simulator Program Policy and Procedures.

c. Scope. This plan is applicable to threat simulators and targets which are used to represent a specific threat system or portion of a specific threat system in Technical and User tests. Laboratory simulators will be validated and accredited if they represent a part or function of a specific threat system and are used in a Technical or User Test supporting a milestone decision. Exceptions to the validation process will be addressed on an individual basis.

d. Validation/Accreditation Support to Materiel Development. Figure 1-1 illustrates the relation of validation and accreditation to the life cycles of Army materiel and threat simulators/targets. As shown in the figure, validation is performed at critical points throughout the life cycle of threat simulators/targets while accreditation pertains to specific test applications of threat simulators/targets during the operational phase of the life cycle of threat simulators/targets. The processes of validation are used to assist development and management of threat simulators/targets.

e. Definitions. The following definitions are Army unique to meet the Army's validation and accreditation mission. They differ slightly from those in DoD 5000.3-M-6 found at enclosure 4.

(1) Accreditation. The examination of validation documentation to determine if a target or threat simulator is an adequate representation of the threat for a given test.

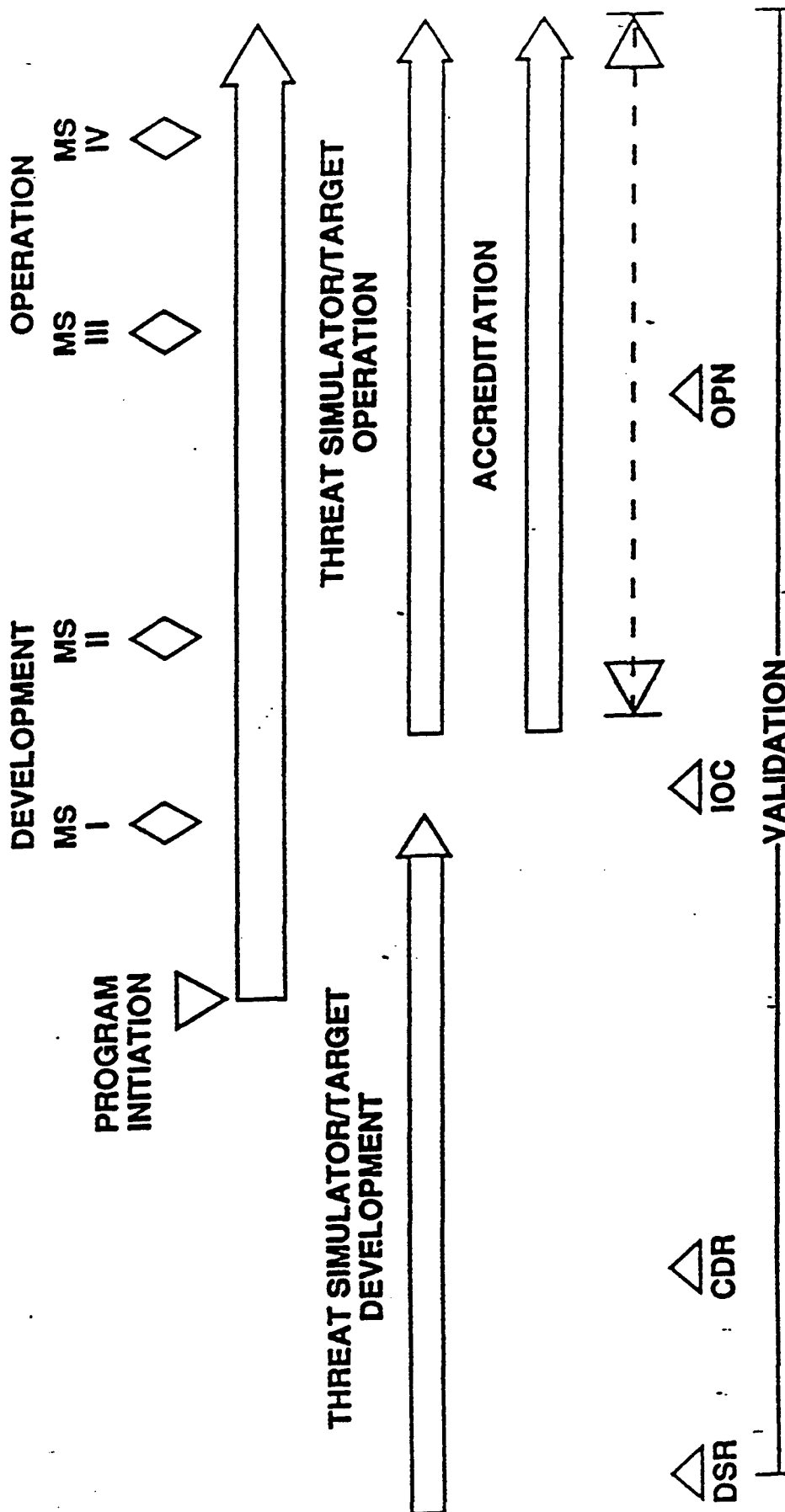
(2) Target. Device which is intended to be engaged and destroyed by blue systems:

(a) Drone Target: An air or ground target converted to remote control for use in testing and training.

(b) Ground Target: A target which is intended to represent an adversary ground vehicle system or ground based military structure for use in testing and training.

VALIDATION/ACCREDITATION SUPPORT TO MATERIEL DEVELOPMENT

ARMY MATERIEL LIFE CYCLE



DSR - DESIGN SPECIFICATION REVIEW
 CDR - CRITICAL DESIGN REVIEW
 IOC - INITIAL OPERATIONAL CAPABILITY
 OPN - OPERATIONAL

Figure 1-1

(c) Aerial Target: A target which is intended to represent an adversary aircraft for use in testing and training.

(3) Threat Simulator. A generic term used to describe a family of equipment used to represent adversary systems in testing and training. A threat simulator has one or more characteristics which replicate the adversary system with a prescribed degree of fidelity.

(4) Validation. The process of comparing simulators and targets to DIA approved threat data and documenting the variations between the simulator/target and the approved threat.

f. References.

(1) DoD 5000.3-M-6, Threat Simulator Program Policy and Procedures dated April 1989.

(2) AR 381-11, Threat Support to U.S. Army Force, Combat, and Materiel Development dated 12 March 1986.

(3) Army Development and Acquisition of Threat Simulators (ADATS) Program Management Plan (PMP) dated 8 July 1988.

(4) Army Target Program Management Plan (PMP) dated January 1990.

(5) AR 73-1, Test and Evaluation Policy and Procedures (Draft).

g. Publication.

(1) Revision, coordination, and publication of this plan will be accomplished by the Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS) and its designated representative. This plan will be updated annually.

(2) Comments, proposed changes, or suggested improvements to this plan should be forwarded on DA Form 2028 (Recommended Changes to Publications) through channels to:

Headquarters, Department of the Army
Deputy Chief of Staff for Operations and Plans
ATTN: DAMO-FDT
Washington, DC 20310-0460

2. VALIDATION

a. General. Validation is the process used to ensure that a given threat simulator or target provides a sufficiently realistic representation of the threat. Validation provides the analysis necessary to justify continuation of development or use, or modification to achieve or restore a sufficiently realistic representation. Threat simulators and targets are developed in order to portray threat systems for user identified test requirements. Accordingly, threat simulators and targets may duplicate or represent a limited number of the attributes of the threat system. Validation must, therefore, be based upon expert knowledge of the threat, the simulator or target, and generic test requirements. Validation will be documented and reported via a threat simulator or target Validation Working Group (VWG). Validation will occur at the key decision points in the threat simulator/target life cycle listed below and depicted in Figure 2-1:

(1) Design Specification Review (DSR). (Note: EXCOM approval required prior to contract award)

(2) Critical Design Review (CDR). (Note: EXCOM notification required)

(3) Initial Operational Capability (IOC). (Note: EXCOM approval required prior to use in testing)

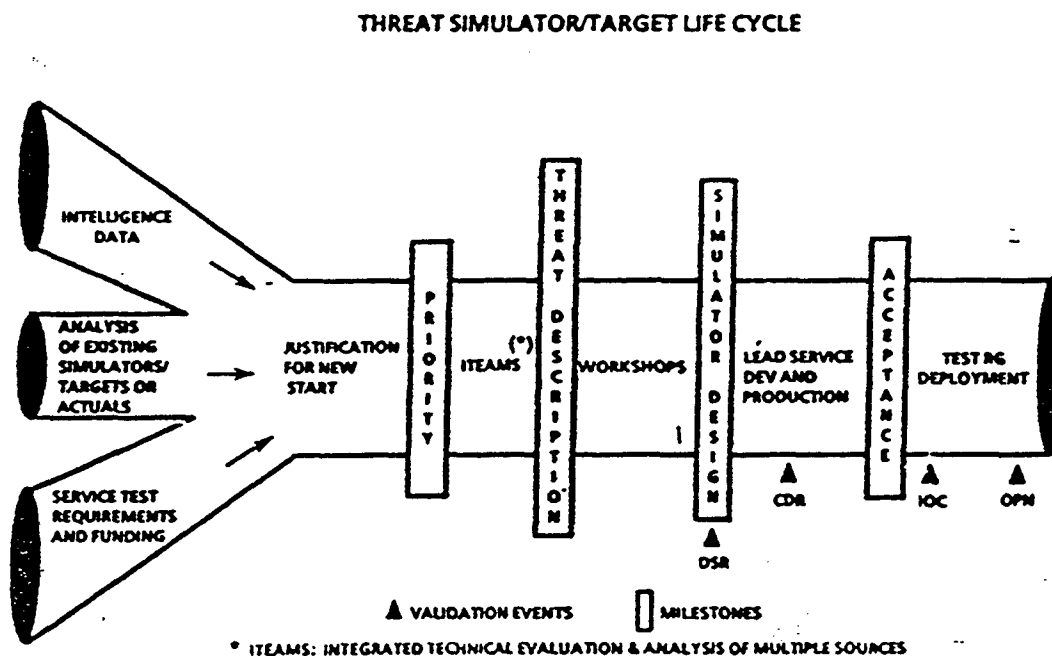


FIGURE 2-1

(4) Upon major modification which affects simulator fidelity and periodically following deployment (operational - OPN). (Note: EXCOM notification required)

b. Responsibilities.

(1) HQDA.

(a) Provide overall DA-level program direction, guidance, review, and approval authority through the General Officers' Steering Council (GOSC). (DCSOPS/TEMA)

(b) Charter VWGs and appoint VWG chairman as required. (TEMA)

(c) Review and approve threat simulator/target requirements. (GOSC)

(d) Approve and transmit copies of validation reports with appropriate forwarding or notification letters to the CROSSBOW-S and DoD Executive Committee on Threat Simulators (EXCOM) as required. (TEMA)

(2) TRADOC

(a) Identify and document threat simulators and target requirements to support combat development efforts.

(b) Participate in VWG as required.

(c) Function as a signatory on validation reports for threat simulators and targets as required.

(3) Army Materiel Command (AMC)

(a) Identify and document threat simulator and target requirements to support technical testing.

(b) Participate in VWG to accomplish Use Analysis as required. (TECOM, AMSAA, LABCOM, RD&E centers, MICOM)

(c) Function as a signatory on validation reports for threat simulators and targets for use in support of Technical Testing as required.

(d) Assist and support in the measurement of threat simulators and target parameters required for validation. These measurements will be subject to S&TI (AIA) approval.

(4) Operational Test and Evaluation Command (OPTEC).

(a) Identify and document threat simulator and target requirements to support user testing.

(b) Participate in VWG.

(c) Function as a signatory on validation reports for threat simulators and targets for use in support of User Testing.

(d) Assist and support in the measurement of threat simulators and target parameters required for validation. These measurements will be subject to S&TI (AIA) approval.

(5) Army Intelligence Agency (AIA).

(a) Participate in VWG. (AIA, MSIC, FSTC, ITAC, TSPO)

(b) Perform or supervise measurement of threat simulator and target parameters as required for comparison to the current DIA approved Scientific and Technical Intelligence (S&TI) center estimates for the threat system. When available, AMC and OTECOM measurement capabilities for targets and threat simulators will be utilized. (AIA)

(c) Perform and document required Technical Analysis (there will be an organizational difference between the functions of validation and development) for threat simulators and targets at key decision points in the life cycle. (MSIC or FSTC)

(d) Function as a signatory on validation reports for threat simulators and targets. (AIA)

(6) Project Manager Instrumentation, Targets, and Threat Simulators (PMITTS)

(a) Maintain a data base on all validation actions. This data base will serve as the official suspense file for all validation actions.

(b) Notify TEMA when validations are due so that VWGs can be established. This should be accomplished at least two quarters prior to the scheduled validation start date.

(c) Participate in VWG.

(7) Test and Evaluation Management Agency (TEMA)

(a) Utilizing the list of required validations submitted by PM ITTS, notify the Defense Intelligence Agency (DIA) through the CROSSBOW-S Committee to task the appropriate S&TI Center to prepare the necessary updated threat data (Standard Validation Criteria) for the validation(s) and to forward the data to the appropriate VWG.

(b) As the Army Representative to the OSD CROSSBOW-S and Excom Committees, monitor DIA and S&TI Center(s)

reports to insure updated threat data are available at the appropriate time for VWG use.

(c) Prioritize all Army requests to DIA for Validation Threat Data.

(d) Charter all VWGs and appoint the Chairman.

c. Validation Process. Validation requires Technical Analysis and Use Analysis. Technical analysis will be performed by the appropriate S&TI Center with the cooperation of the material developer. A Technical Analysis Report (TAR) will be developed and forwarded to the VWG for review, analysis and implementation. Technical and Use Analysis are explained below and graphically portrayed in figure 2-2.

(1) Technical Analysis. Technical analysis compares the technical characteristics and capabilities of a threat simulator or target to current Defense Intelligence Agency (DIA) approved intelligence concerning the related threat system. The TAR will define the agreement and differences between the simulator/target and the threat, and state the implications of the differences for the technical capabilities of the simulator/target. Technical analysis will use data developed jointly by the technical analysis organization and the simulator/target developer to satisfy standard validation criteria from the DoD Executive Committee on Threat Simulators (EXCOM). The responsible S&TI Center will issue the TARs to the Validation Working Groups (VWGs).

(2) Use Analysis. Use analysis compares the capabilities and limitations of the threat simulator or target described in the TAR with the projected general use to determine the utility of the simulator/target. The membership of the Validation Working Group will combine the knowledge of the simulator/target, threat, and use to evaluate the capabilities and limitations, and determine the validity of the simulator/target for its intended role.

d. Validation Decision Points. Validation must be accomplished at the threat simulator/target life cycle key decision points listed below to comply with Department of Defense Manual DoD 5000.3-M-6.

(1) Design Specification Review (DSR). Validation of the design specification establishes a means for and a formal record of the evaluation of the threat simulator/target design, the current intelligence regarding the threat system, and the intended use of the device. EXCOM approval is required. This validation is conducted prior to issuance of the contract for simulator development or for purchase of foreign equipment for use in testing.

(2) Critical Design Review (CDR). Validation of the design approved during the CDR provides a comparison of the latest intelligence, the simulator/target design, and the level of

Red Threat Technical Analysis

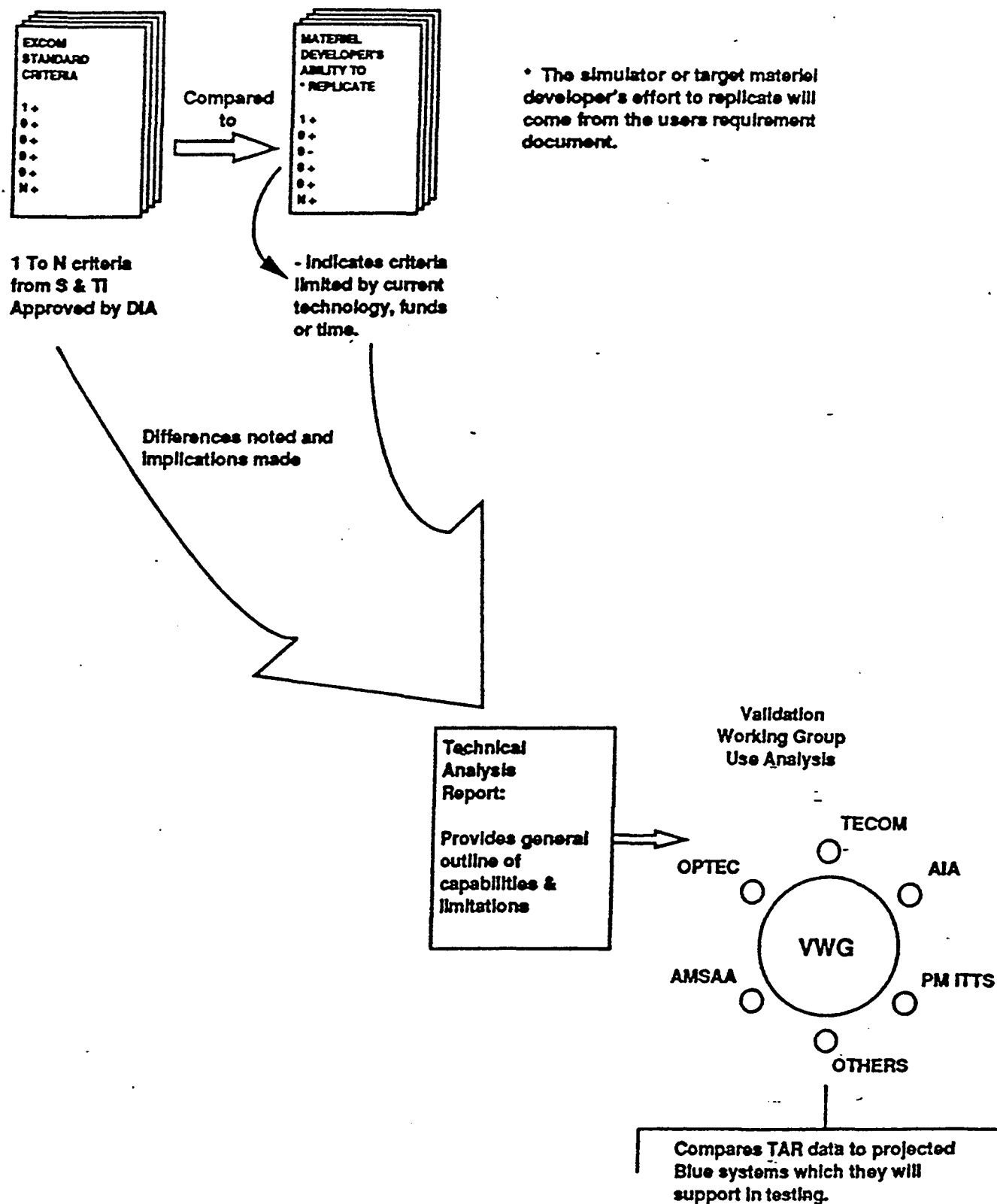


Figure 2-2

fidelity required by the planned use. This validation documents the comparison for all audit purposes and may serve to support decisions concerning funding or other resources required for development. EXCOM notification is required.

(3) Initial Operational Capability (IOC). Validation at IOC provides the first opportunity to compare the complete, functional threat simulator/target, current intelligence estimates of the threat system, and the planned use of the device. This validation is used to support the fielding decision and documents the performance of the threat simulator/target for test planning and audit purposes. EXCOM approval is required prior to use in testing.

(4) Operational (OPN). Validation is accomplished on threat simulators and targets after modification and periodically throughout their operational life to ensure their capability to represent threat systems as described by current intelligence estimates. Operational validation consists of comprehensive testing and analysis of performance, configuration, and fidelity to current threat estimates. EXCOM notification is required.

e. Validation Working Group (VWG). VWGs will evaluate and report on threat simulators and targets at the key decision points in the life cycle outlined above.

(1) Establishment. A VWG will be established and chartered for each threat simulator or target for each validation decision point. The Test and Evaluation Management Agency (TEMA), Headquarters, Department of the Army (HQDA) will charter VWGs based on schedules provided by PM ITTS. The charter will designate the chairman and the organizations responsible for the validation.

(2) Organization. VWGs will be composed of representatives from the responsible user, intelligence, and simulator/target development organizations. Representatives from the following organizations will participate in VWGs as indicated:

(a) Test and Evaluation Command (TECOM). Mandatory membership.

(b) Operational Test and Evaluation Command (OTECOM). Mandatory membership.

(c) Army Intelligence Agency (AIA). Mandatory membership.

(d) Army Materiel Systems Analysis Activity (AMSAA). Mandatory membership.

(e) Project Manager Instrumentation, Targets and Threat Simulators (PM ITTS). Mandatory membership.

(f) AMC Laboratory Command (LABCOM). As required.

(g) AMC Research, Development, & Engineering Centers (RD&E Centers). As required.

(h) Missile and Space Intelligence Center (MSIC). As required.

(i) Foreign Science and Technology Center (FSTC). As required.

(j) Training and Doctrine Command (TRADOC). As required.

(k) Other Army organizations. As required.

(l) Other Service representatives. As required.

(3) Functions. General functional areas of specific member organizations are outlined in Figure 2-3. Figure 2-4 illustrates the events involved in validation. The functions and responsibilities of VWGs are itemized below:

(a) Consolidate critical threat parameters and tolerances (e.g. Threat Specification Packages (TSP) produced by the Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS); threat specifications and completed EXCOM approved standard validation criteria validated by DIA).

(b) Develop validation program plans to collect data and produce the analysis required for validation.

(c) Oversee collection of validation data. Serve as a forum for resolution of issues.

(d) Determine and assess the effects of the differences between the simulator/target and DIA approved intelligence.

(e) Recommend acceptance or modification to produce adequate representation of the threat to DCSOPS/TEMA.

(f) Submit required validation report (enclosure 2) for approval (at DSR and IOC) and for notification, information, and retention (at CDR and OPN) through the CROSSBOW-S to the DoD Executive Committee on Threat Simulators (EXCOM). A letter of transmittal forwarding the Validation Report will be used. A sample is at Appendix 1 of enclosure 2.

(g) As part of the Initial Operational Capability (IOC) validation for each system, The IOC Validation Working Group (VWG) will specify the interval (when) and the Data/Criteria from the Threat Definition Document (TDD) that will be used in the operational validation. The operational validation interval and criteria (when and what TDD data) will be included as part of the IOC Validation Report. The TDD data to be used in the OPN Validation will be called the "Critical Criteria".

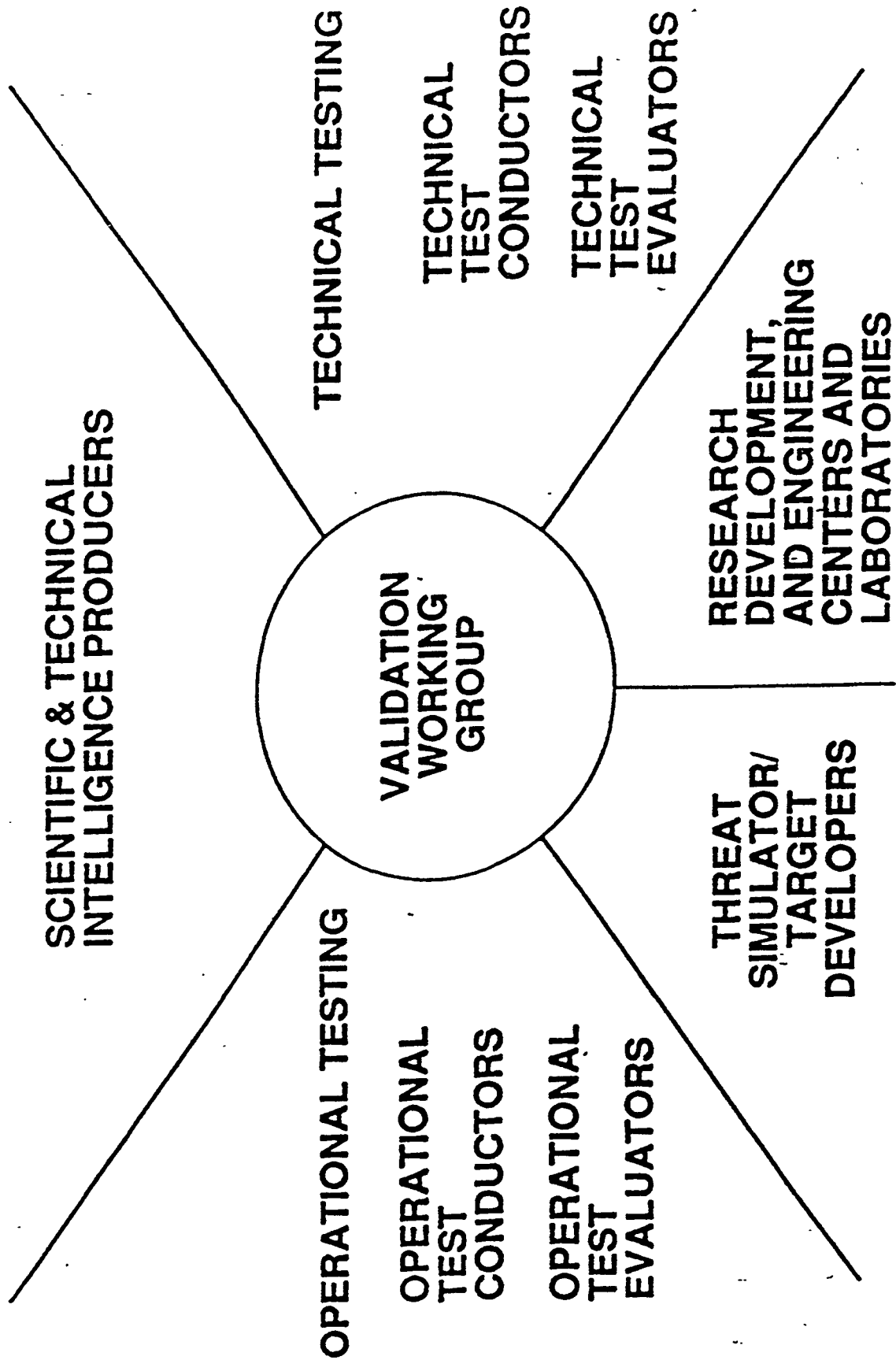


Figure 2-3
Validation Working Group Membership

VALIDATION EVENT CYCLE

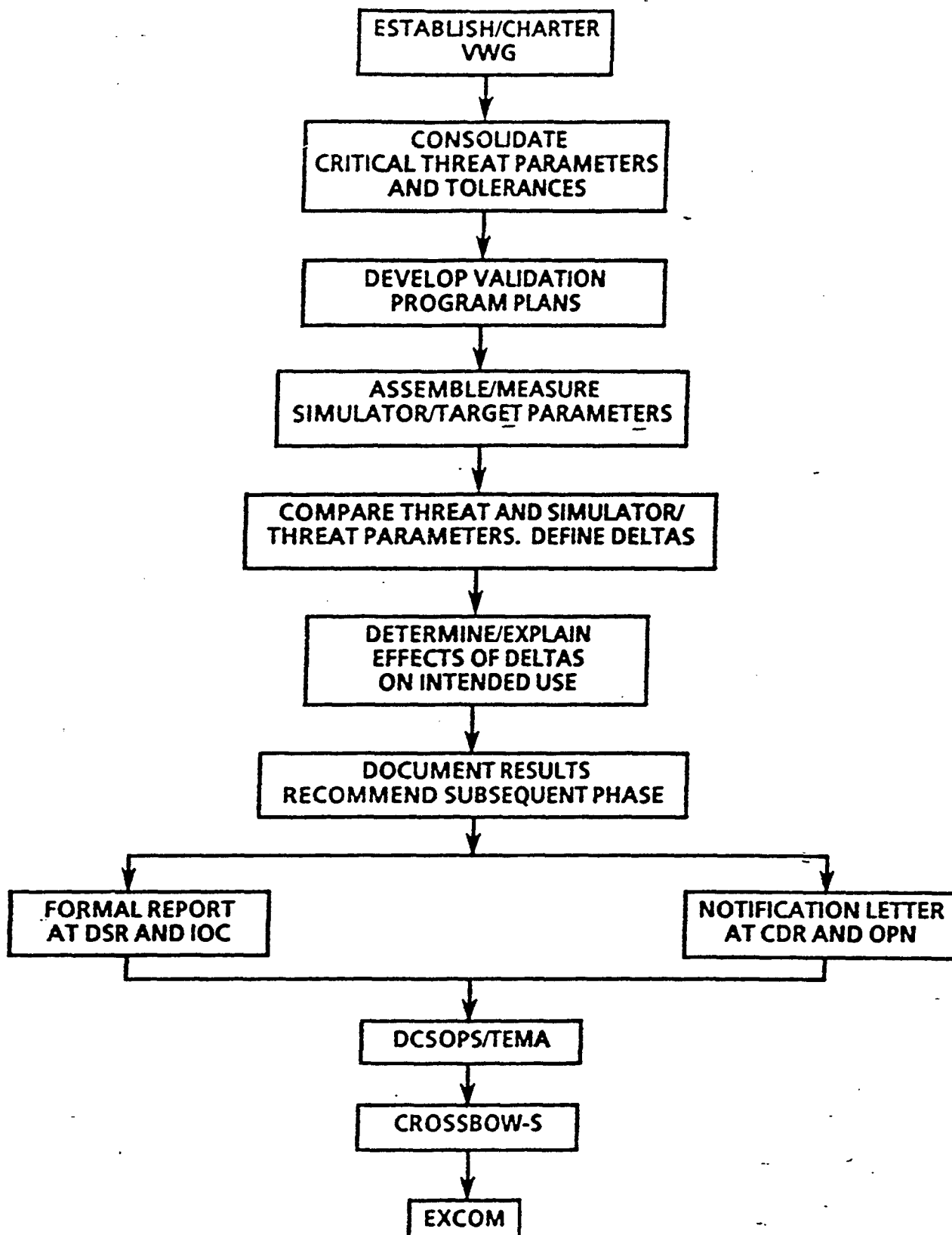


FIGURE 2-4

(h) Targets and threat simulators developed and fielded prior to the implementation of DoD validation procedures (DoD 5000.3-M-6) were grandfathered from the developmental validation process i.e. DSR, CDR, and IOC. They are however, subject to the provisions for operational validation. For those systems, OPTEC and AIA (for threat simulators) and TSO and AIA (for targets) will jointly determine the future OPN validation cycle. The resulting schedule will be furnished to PM ITTS, who will coordinate with TEMA, the establishment of OPN VWGs. For Grandfathered systems, the initial OPN VWG will determine what TDD data (i.e. critical criteria) will be used in the OPN validation.

(i) The OPN VWG established to manage the OPN validation will meet at least two quarters prior to the scheduled OPN Validation to determine the location for the conduct of the OPN Validation. VWG will base its decision on a thorough review of changes in the threat and other pertinent factors that may impact on the amount of effort involved in conducting the Operational Validation. The Validation Working Group will direct the most convenient, least disruptive to testing and least expensive location to conduct the Operational Validation (locations may be TSPO, OTSA, a combination, AMC facility, ETC.).

3. ACCREDITATION

a. General.

(1) Accreditation is the process used to assess whether threat simulators and targets are suitable for specific tests. Accreditation is accomplished and documented under the auspices of the Test Integration Working Group (TIWG). The Test and Evaluation Master Plan (TEMP) will be the basic document used to record threat simulator and target accreditation. Threat simulator /target and test usage requirements will be identified in paragraph 5, "Test Targets" of "Part V, Test and Evaluation Resource Summary" of the TEMP for the program of interest. These paragraphs will describe test limitations resulting from any differences between the threat simulator or target and the designated threat.

(2) In accreditation, the data requirements of a particular test are compared to the latest intelligence and to the capabilities of Army threat simulators and targets as shown in the current validation reports. Differences between the threat simulators or targets and the intelligence concerning the capabilities of the relevant threat system are analyzed, and assessed against the critical test criteria. These differences must also be assessed against the Critical Intelligence Parameters (CIP), defined in AR 381-11, to determine whether the performance characteristics and capabilities of the simulator and/or target representing the threat are within the established CIPs. Differences, particularly those exceeding the CIPs, which cannot be accommodated or offset in test planning, are defined and assessed to justify modification of the simulators/targets, or acquisition of alternate simulators or targets. Differences assessed to be outside the CIPs may be identified for critical impact on the effectiveness, survivability, and cost of the U.S. system under development.

(3) Threat accreditation is essential for the following reasons:

(a) Any difference between threat simulators and targets and the corresponding threat systems can prevent adequate representation of the threat in a particular test. Even the differences accepted during development and validation can make the simulator or target incapable of adequately representing the threat in a particular test.

(b) The intelligence concerning threat systems is dynamic. New intelligence can make a simulator or target invalid for a given test.

(c) Threat simulators and targets experience deterioration and failures which can make them unable to represent the threat. Accreditation decisions must, therefore, be based on current assessment of the performance of the simulators/targets.

(4) Accreditation is required prior to the use of a threat simulator or target and must be incorporated into the planning and preparation for tests. The accreditation process, in addition to accrediting simulators and/or targets for each use, complements the function of the TIWG to improve test planning, specifically defines test resource requirements for the Outline Test Plan (OTP), and provides guidance for further refinement of the Threat Test Support Package.

b. Responsibilities.

(1) Headquarters, Department of the Army (HQDA).

(a) Maintain, review, and validate critical intelligence parameters (CIP) that affect the effectiveness, survivability, or security of U.S. systems. (DCSINT)

(b) Designate Threat Integration Staff Officers (TISO) for MDAP, ADAP, and DOT&E oversight systems. (DCSINT)

(c) Coordinate with the DCSINT for the integration of Army-approved threat in test programs, including operational testing (OT), force development testing and experimentation (FDTE), and joint operational testing. (DCSOPS)

(d) Coordinate and review threat support for Technical and User testing to include use of scenarios and simulators (i.e., OTSA). (TCG)

(e) Participate in TIWG and Threat Accreditation Working Groups (TAWGs). Chair TAWGs for major programs and non-major programs on the DOT&E oversight list. (TISO)

(2) U.S. Army Training and Doctrine Command (TRADOC) will provide critical issues and criteria for the use of the TIWG/TAWG. (HQ TRADOC or TRADOC School)

(3) Army Materiel Command (AMC).

(a) Ensure the integration of approved threat in technical test programs.

(b) Participate in TIWG and TAWG as required. (appropriate AMC activities)

(c) Provide critical technical issues and criteria and test/threat scenarios to the TAWG for its use in assessing threat simulator/target suitability/adequacy. (AMSAA)

(d) Provide target and threat simulator technical and performance data for use by the TAWG in assessing threat simulator/target suitability/adequacy. (appropriate AMC activity)

(4) Operational Test and Evaluation Command (OTECOM).

(a) Coordinate test planning with the appropriate threat approval authority to ensure that an appropriate battlefield environment is portrayed.

(b) Participate in TIWG and TAWG as necessary.

(c) Provide critical operational issues and criteria and test/threat scenarios to the TAWG for its use in assessing threat simulator/target suitability/adequacy.

(5) Army Intelligence Agency (AIA).

(a) Participate in TIWG and TAWG. Chair TAWG for non-major systems or delegate to the appropriate OT or TT organization. (FSTC, MSIC, TSPO, and/or ITAC)

(b) Provide current Threat Simulator Validation Report for use by the TAWG in assessing threat simulator/target suitability/adequacy. (FSTC, MSIC, TSPO, and/or ITAC)

(6) U.S. System Program Managers (PM).

(a) Establish Test Integration Working Groups (TIWG) for development/coordination of Test and Evaluation Master Plans (TEMP) and coordination of plans for individual tests.

(b) Provide U.S. system technical data for use by the TAWG in assessing threat simulator/target suitability/adequacy.

(c) Participate in TAWG to refine threat simulator and target requirements.

(d) Fund those activities required to accredit threat simulators and targets for a given test or test activity.

(e) Provide administrative support to TAWG.

c. Threat Accreditation Working Group (TAWG). TAWGs will assess, document, and report on threat simulator/target suitability/adequacy in support of specific tests:

(1) Establishment. A TAWG will be established under the auspices of the TIWG for each test anticipating use of threat simulators/targets.

(2) Organization. TAWGs will be composed of representatives from the responsible user, intelligence, and threat simulator/target development/operation organizations. The chairman and membership will be in accordance with the Accreditation Responsibilities section above. Representatives of the following organizations will participate as required:

- (a) Headquarters, Department of the Army.
(DCSINT/TISO)
- (b) U.S. Army Training and Doctrine Command
(TRADOC).
- (c) U.S. Army Operational Test and Evaluation
Command (OPTEC).
- (d) Test and Evaluation Command (TECOM).
- (e) Army Materiel Systems Analysis Activity
(AMSAA).
- (f) Foreign Science and Technology Center (FSTC).
- (g) Missile and Space Intelligence Center (MSIC).
- (h) Intelligence and Threat Analysis Center
(ITAC).
- (i) Threat Simulator Project Office (TSPO).
- (j) Project Manager Instrumentation, Targets and
Threat Simulators (PM ITTS).
- (k) OPTEC Threat Simulator Activity.
- (l) Laboratory Command.

(3) Functions. General functional areas for organizations are outlined in Figure 3-1. The Accreditation Event Cycle is depicted in Figure 3-2. Functions and responsibilities of the TAWG as a body are itemized below.

(a) Threat Accreditation Working Groups (TAWGs) will be established (and chaired) by the DCSINT for MDAP, ADAP, and DOT&E oversight systems. TAWGs will be established and chaired for non-major systems as discussed above. The purpose of TAWGs is to determine the ability of the simulators/targets proposed for a test to represent the relevant threat characteristics needed during that test.

(b) The test data requirements will be analyzed to develop the accreditation plan including any additional requirements for simulator/target data and measurements.

(c) The TAWG will examine the test data requirements, threat data analysis, and the simulator/target validation data to determine the ability of the simulators/targets to represent the relevant threat system characteristics.

(d) Document, via letter report to the TIWG, the suitability of the individual threat simulators/targets for use in

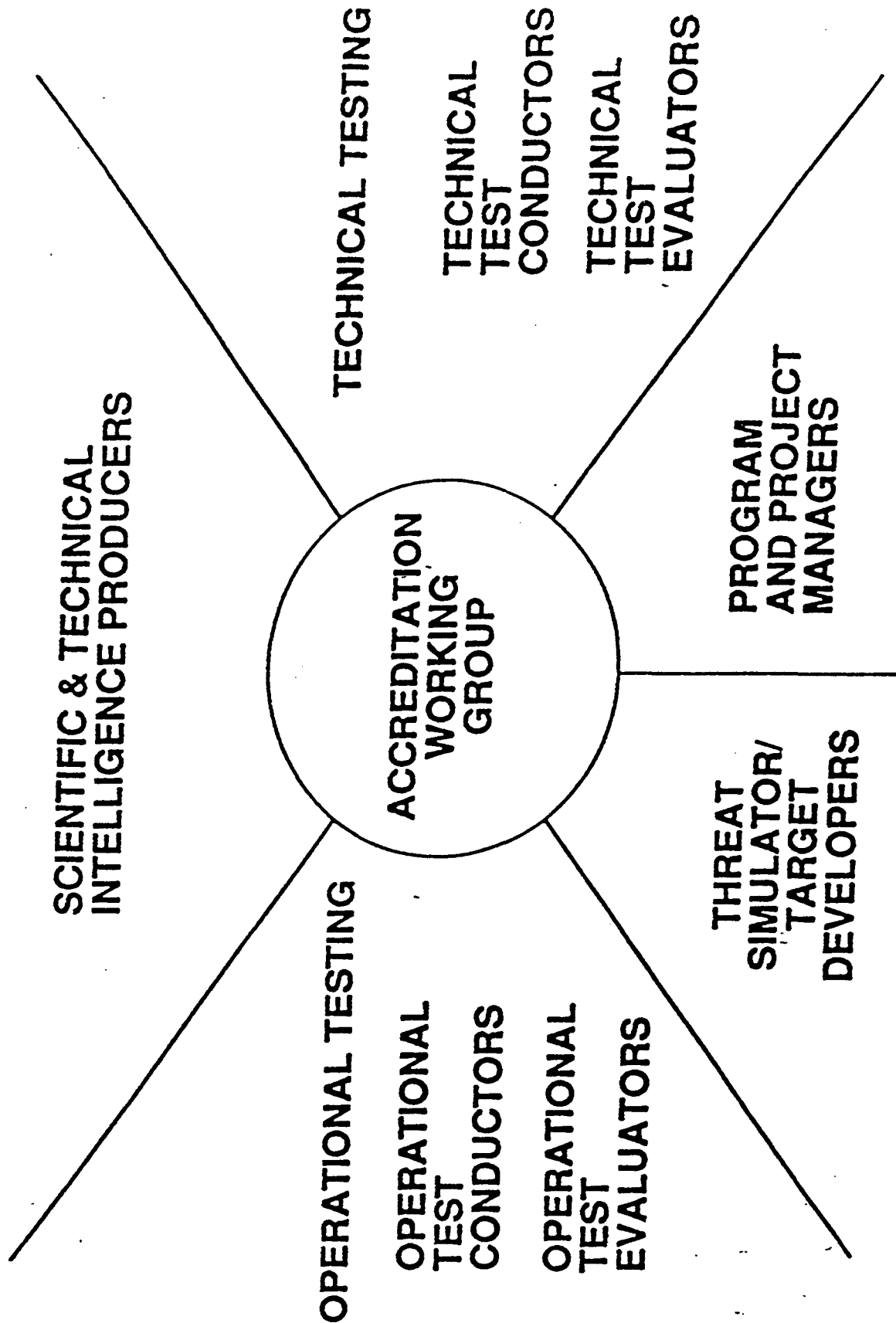


Figure 3-1
Accreditation Working Group Membership

ACCREDITATION EVENT CYCLE

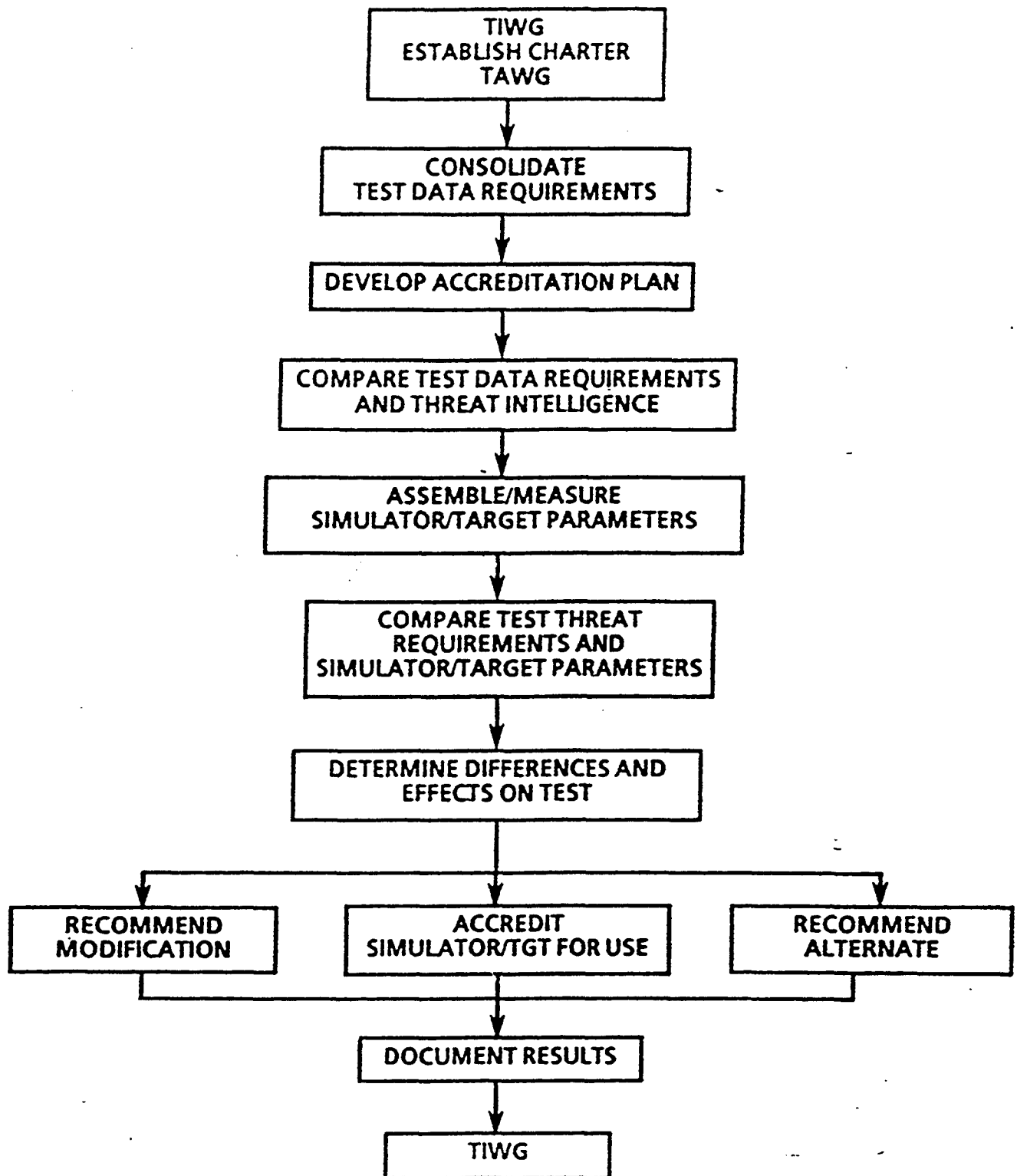


FIGURE 3-2

support of the specified test under consideration. A summary of the findings will be included in the TEMP.

(e) An accreditation report at enclosure 3 will be used as the summary of findings in para.(d) above. A letter of transmittal will be used. A sample is at appendix 1 of enclosure 3.

ABBREVIATIONS AND ACRONYMS

ADAP	Army Designated Acquisition Program
ADATS	Army Development and Acquisition of Threat Simulators
ADATS-A	ADATS-Activity
AIA	Army Intelligence Agency
AMC	Army Materiel Command
AMSAA	Army Materiel Systems Analysis Activity (AMC)
CAC	Combined Arms Center (TRADOC)
CATA	Combined Arms Training Activity (TRADOC)
CDR	Critical Design Review
CIP	Critical Intelligence Parameter
CROSSBOW-S	Construction of a Radar to Operationally Simulate Signals Believed to Originate Within the Soviet Union
DCSCD	Deputy Chief of Staff for Combat Developments (TRADOC)
DCSI	Deputy Chief of Staff for Intelligence (HQDA)
DCSINT	Deputy Chief of Staff for Intelligence (TRADOC)
DCSOPS	Deputy Chief of Staff for Operations and Plans (HQDA)
DCST	Deputy Chief of Staff for Training (TRADOC)
DIA	Defense Intelligence Agency
DIR	Director(ate)
DoD	Department of Defense
DOT&E	Director of Test and Evaluation (DoD)
DSR	Design Specification Review
EXCOM	DoD Executive Committee on Threat Simulators
FDTE	Force Development Test and Experimentation
FSTC	Foreign Science and Technology Center (AIA)
GOSC	General Officer Steering Committee
HQDA	Headquarters, Department of the Army
IOC	Initial Operational Capability
IPR	In-Process Review
ITAC	Intelligence and Threat Analysis Center (AIA)
ITEAMS	Integrated Technical Evaluation and Analysis of Multiple Sources
MACOM	Major Command
MATTS	Office for Management of Targets and Threat Simulators (TECOM)
MDAP	Major Defense Acquisition Program
MICOM	Missile Command (AMC)
MSIC	Missile and Space Intelligence Center (AIA)
OPN	Operational
OT	Operational Test(ing)
OT&E	Operational Test and Evaluation
OTEA	Operational Test and Evaluation Agency
OTP	Outline Test Plan
PM	Program/Project Manager
PM ITTS	Project Manager Instrumentation, Targets and Threat Simulators
PMP	Program Management Plan
PROJ OFC	Project Office(r)
RAM	Reliability, Availability, and Maintainability

S&TI	Scientific and Technical Intelligence
TAWG	Threat Accreditation Working Group
TCG	Threat Coordination Group
TECOM	Test and Evaluation Command (AMC)
TEMA	Test and Evaluation Management Agency (HQDA)
TEMP	Test and Evaluation Master Plan
TEXCOM	Test and Experimentation Command (TRADOC)
TISO	Threat Integration Staff Officer
TIWG	Test Integration Working Group
TMO	Targets Management Office (MICOM)
TRADOC	Training and Doctrine Command
TSPO	Threat Simulator Project Office (MSIC)
TT&E	Technical Test and Evaluation
TTSP	Test Threat Support Package
TWG	Target Working Group
UT	User Test(ing)
UT&E	User Test and Experimentation
VWG	Validation Working Group

Enclosure 1 (Accreditation Responsibilities)

1. Office of the Deputy Chief of Staff, Intelligence (ODCSINT).

- a. Represent the DCSINT at TIWGs and TAWGs.
- b. Function as the "honest broker" for the DCSINT when providing threat assessments.
- c. Support the TIWG and TAWG chairman through their respective Foreign Intelligence Officers (FIO) and TRADOC Threat Managers (TM). To this end, the TISO will:

- (1) Identify and report threat-related issues impacting upon program execution.
- (2) Monitor and report status of threat documentation (e.g. STAR, TTSP, AIA taskers).
- (3) Respond to threat-related queries and questions beyond the capacity of supporting TMs and FIOs.
- (4) Coordinate DIA validation of threat assessments, as required.

2. U.S. System Program Manager (PM).

- a. Establish and chair TIWGs for development and coordination of TEMP.
- b. Provide U.S. system technical data for use by the TAWG in assessing threat simulators or target suitability.
- c. Participate in TAWG to refine threat simulators, targets and target arrays.
- d. Fund those activities required to accredit threat simulators and targets for a given test or test activity.
- e. Provide administrative support to the TAWG.

3. Operational Test and Evaluation Command (OPTEC).

- a. Participate in TIWG.
- b. Chair TAWG.
- c. Coordinate test planning with the appropriate TRADOC TM or AMC FIO to ensure that an appropriate battlefield environment is portrayed.

d. Provide critical operational issues and criteria and test scenarios to the TAWG for use in assessing simulators, targets and target array suitability.

4. Project Manager Instrumentation, Targets, and Threat Simulators (PMITTS).

a. Participate in TIWG, VWG, and TAWG.

b. Maintain data base on all validation actions to provide status of simulator validation to the TAWG to include number of simulators and signature validated to date.

5. Foreign Science and Technology Center (FSTC).

a. Participate in Validation Working Group (VWG) and TAWG.

b. Provide signature measurements of actual targets to be used for comparison with threat simulators.

c. Provide assessment, as member of VWG, of the differences between targets and simulators to be used during testing.

d. Provide advice and technical assessments during accreditation process.

6. Intelligence and Threat Analysis Center (ITAC).

a. Participate in TAWG, as requested.

b. Provide target array assessments, when requested.

7. U.S. Army Materiel Systems Analysis Activity (AMSAA).

a. Participate in TIWGs and TAWGs.

b. Provide critical technical issues and criteria and test scenarios to the TAWG for its use in assessing simulator or target suitability.

8. Laboratory Command (LABCOM).

a. Participate in VWG and TAWG, as required.

b. Assist and provide measurements, as a member of the VWG, of threat simulators and target parameters required for validation and comparison with actual target measurements.

c. Provide advice and technical assessments of differences between targets and simulators during accreditation process.

Appendix B

Detailed Test Plan Outline

Reference. The source for the information in this appendix is:

TECOM PAM 73-1 (Draft): Technical Test and Assessment Guide, TECOM,
May 1992.

SECTION 1. INTRODUCTION

1.1 TEST OBJECTIVE

The objective of the test is a statement of the overall purpose of the testing actions. It should be a restatement of the objective from the test directive or, for customer tests, from the test request. It is a general answer to the question "Why is the test effort being performed?"

1.2 TESTING AUTHORITY

The testing authority will identify and reference the:

- a. Test directive, specifying the test center(s) involved and stating the type of test (e.g., TFT, PQT).
- b. Test request, specifying the PM sponsoring this testing.

1.3 TEST CONCEPT

Present an overview of the concept of test (location(s), duration, timeframe, type(s) of subtests, numbers of test items, etc.). Cite sufficient detail to allow the reader to clearly understand the extent of testing. Address special test considerations required such as known limitations. This paragraph should directly relate to the IEP and the Integrated Test Schedule of the TEMP, and should be an updated restatement of the test concept from the directive.

1.4 SYSTEM DESCRIPTION

The description is derived from the IEP, TEMP, or other source documents. It should describe the test item in terms of function, technical parameters, physical characteristics, mission, and threat. If the test item consists of several major components, identify these and describe each. If test items differ from previously tested items, describe the differences in the test items.

If literature on the test item exist, include appropriate extracts of the description and cite the reference. Ensure that the manufacturer's performance claims are not included as facts in the description. Listing physical characteristics rather than performance information or identifying them as unproven claims or required characteristics will avoid this.

This description must permit full understanding of the item. Include a line drawing or photograph, if available.

1.5 UNIQUE TEST PERSONNEL REQUIREMENTS

Describe the use of SOMTE personnel in terms of critical operator and maintainer tasks (see TECR 70-5).

Describe whether or not personnel qualified to test by duty assignment will be used (see TECR 70-25).

SECTION 2. SUBTESTS

This is the most important section of the test plan. Include specific subtests necessary to provide test data to answer the assessor's Critical Technical Parameters, and/or to describe the degree to which an item meets the criteria specified in requirements, TECOM directives, military standards, military specifications, etc.

State what is being measured and how the test will be accomplished. When appropriate, reference applicable elements from the IEP or TECOM directive.

Keep the subtest limited in scope. Generally, the criteria are the guide for subtest partitioning. A short subtest discussing only one specific topic is easier to write and read. Longer subtests may be divided into subelements. For example, a human factors subtest may be divided into workspace, visual, noise, lighting, etc.

For subtests to be satisfied by contractor/developer testing which are described in a published contractor/developer test plan, for which the test manager has assigned certain responsibilities to the test center (e.g., data analysis, data reduction, or on-site monitoring), ensure that complete information on that subtest is provided. Describe all elements for that subtest from the externally prepared document and delineate the responsibilities of the test center.

Include sufficient detail to enable approving authorities to determine if the scope of the specific subtests will accomplish the subtest objective, determine the justification for conducting the subtests, and to allow a tester other than the plan's author to conduct the test.

Paragraph headings and contents for this section are as follows:

2.1 NAME OF SUBTEST

2.1.1 OBJECTIVES

The objectives of the subtest should support the test objectives (para 1.1). State the objective or reason for conducting the subtest in a brief statement; e.g., "Determine the reliability of the (system)."

2.1.2 CRITERIA

State the criteria verbatim from its sources. State source and paragraph in parentheses following the criteria. The criteria may be derived from the IEP, requirements documents, test directive, regulations, standards, and/or operating procedures.

The criteria should be quantitative where possible, but qualitative criteria is acceptable if the circumstances do not lend themselves to numerical values. The criteria should be stated so they may be considered in terms of met, partially met, or not met.

For a subtest with no criteria available, the test director may develop criteria, listing the test center as the source. The approval of the test plan will constitute approval of the subtest criteria. If no criteria would be required (i.e., subtest designed to provide data with no assessment), state "This subtest is conducted to document technical performance."

A complete listing of criteria will be included in Appendix A. In those instances where several criteria would be listed, appendix A of the plan may be referenced in lieu of listing numerous criteria (e.g., "See items 2 through 10, and 17 in Appendix A).

2.1.3 TEST PROCEDURES

The procedures to be used in the subtest should be described in sufficient detail to allow the reader to understand what will occur. If possible, TOPs, ITOPs, or MIL-STDs should be referenced. Describe in sufficient detail how the subtest will be conducted so that another individual knowledgeable in testing of such material could follow the procedure and conduct the test. Describe how the test item will be operated or what it will be exposed to in order to conduct the subtest.

Specify what data will be acquired and how it will be acquired. The what/how pairing will, as a minimum, reflect data requirements expressed in the IEP. Justify stringent data accuracy requirements.

Subparagraphs (e.g., 2.1.3.1, 2.1.3.2) may be used to organize the test procedures to enhance the reader's understanding.

2.1.4 DATA REQUIRED

Include a listing of all data elements that will be recorded during the subtest. Specify the accuracies required for the measurements.

The use of standard forms, data sheets, or questionnaires are encourage. If standard forms, data sheets, or questionnaires are to be used, include as an appendix and reference that appendix.

2.1.5 DATA ANALYSIS/PROCEDURE

Describe how the data are to be analyzed by the test center and how it should be reported. For each criteria, specifically identify in a separate subparagraph how it will be addressed and what condition will lead to a determination that the criteria has been met. Address only that portion of a criterion applicable to the specific subtest.

Present the analytical procedure in the same order that it was introduced in the test procedure paragraph. Specify any compression, reduction, averaging, compilation, and/or statistical treatment. Include any assumptions that are appropriate.

For analytical and/or statistical procedures, the procedure should be identified in sufficient detail to allow another individual to carry out the analysis and to allow a review (test manager, evaluator/assessor, PM, etc.) to judge the adequacy of the methodology. Sufficient detail does not mean the complete equations for computations such as single T-Test, standard ANOVA, or simple point estimate, and confidence limits. Identification of statistical test name, sample size, confidence/or risk levels (whichever is appropriate), and any distribution assumption is sufficient.

Analytical procedures should provide interpretations of criteria statements where necessary.

SECTION 3. APPENDICES

A. TEST CRITERIA

Extract appropriate test criteria verbatim from the IEP, requirements document, contract specification and standards, or other sources. This format will subsequently be used in the test report format with a "Remarks" column added.

Item	Applicable Source	Test criteria	Subtest
------	----------------------	------------------	---------

When a portion of a listed criteria is not to be examined, underline the nonapplicable portion and add the following statement: NOTE: Underlined portion of criteria will not be addressed.

At the end of the criteria, list the Technical Parameters from the Technical Assessor and reference subtests that will provide information on each parameter.

B. TEST SCHEDULE

Provide realistic schedules of the test effort to ensure efficient programming and utilization of resources. Front load tests which provide input for the safety release.

Every effort should be made to minimize the time required to accomplish the test. Prepare an incremental test schedule presenting an estimate of net testing time in a Gantt chart format.

C. INFORMAL COORDINATION

Informal coordination is that coordination effected with a PM or MSC-level or below. Include a list of all agencies with which the draft test plan was informally coordinated. Indicate coordination comments not incorporated into the plan. List the agency providing the comment, the comment and the reason for not accommodating the comment. Major disagreements or anomalies, in the judgement of the test plan preparer, will immediately be brought to the attention of the TECOM test manager.

D. REFERENCES

This appendix should list all documents mentioned in the plan, in the order in which they were mentioned.

E. ABBREVIATIONS

All acronyms, brevity codes, short titles, and abbreviations used in the plan are listed alphabetically with an explanation of their meaning. Do not list commonly used terms.

F. DISTRIBUTION LIST

The distribution list will list all agencies receiving the plan in accordance with the HQ TECOM test directive and internal test-center requirements.

REFERENCES

1. DA PAM 70-21: Research and Development, A Test and Evaluation Guide (Draft), HQDA, August 1990.
2. Captive Flight Test Data Reduction and Analysis Plan (Grayling Winter Deployment), TASC, June 1990.
3. TECOM Environmental Documentation Process Guide, TECOM, undated.
4. AR 200-2: Environmental Effects of Army Actions, HQDA.
5. Range Users Handbook, WSMR, 1991.
6. Smart Weapons Technology Transitions Guide, AMC-SWMO, September 1988.
7. Smart Munitions Test and Evaluation Blue Team/Red Team Final Report Briefing, AMC-SWMO/TECOM Directorate for Technology, April 1991.
8. Smart Munitions Survey of Specialized Test Facilities, AMC-SWMO, January 1988.
9. TECOM PAM 73-1 (Draft): Technical Test and Assessment Guide, TECOM, May 1992.
10. Captive Flight Data Collection Plan (Grayling Winter Deployment), TASC, January 1990.
11. Smart Munitions Evaluation Planning Guide, AMC-SWMO, November 1988.
12. Smart Munitions: Testing During Proof of Principle, AMC-SWMO, February 1988.
13. Government Data Base Sensor Captive Flight Test and Drop Test Plan (Draft), PM SADARM, December 1990.
14. An Army Guide to Live Fire Test and Evaluation, TEMA, August 1990.
15. AR 70-10: Test and Evaluation During Development and Acquisition, HQDA, August 1975.
16. AR 70-1: Systems Acquisition Policy (Interim), HQDA, May 1992.

REFERENCES (CONT)

17. Handbook on Dirty Battlefield Testing of Electro-Optical Systems, MICOM T&E Directorate, May 1990.
18. AR 73-XX: Test and Evaluation Policy, HQDA, November 1990.
19. DA PAM 73-XX: Volume 3, Technical T&E Procedures and Guidelines (Draft), HQDA, April 1992.
20. Smart Munition Model Catalog User's Manual, GACIAC SR-88-17, December 1988.
21. DAMO-FDZ Memo: U.S. Army Validation and Accreditation Plan for Threat Simulators and Targets, HQDA, February 1991.
22. AMC-SWMO Countermeasures Study, Vol II: Effects of Countermeasures on Smart Weapons Technology (U), SECRET, AMC-SWMO, June 1991.
23. TECOM Environmental Documentation Process Guide, TECOM, undated.
24. Weather Specification Guide, AMC-SWMO, 31 October 1990.
25. AMC-SWMO Study Volume I: Guide to How Countermeasures Affect Smart Weapons, AMC SWMO, January 1992.
26. Chicken Little Project Office, TABILS Database, Eglin AFB., FL 32542-5000
27. Discussions with Dick Ehrenreich, Dynetics, 11 Aug 1992.

GUIDANCE AND CONTROL INFORMATION ANALYSIS CENTER (GACIAC)

GACIAC is a DoD Information Analysis Center operated by IIT Research Institute under the technical sponsorship of the Joint Service Guidance and Control Committee with members from OSD, Army, Navy, Air Force, and DARPA. The AMC Smart Weapons Management Office of the U.S. Army Missile Command provides the Contracting Officer's Technical Representative. GACIAC's mission is to assist the weapon guidance and control community by encouraging and facilitating the exchange and dissemination of technical data and information for the purpose of effecting coordination of research, exploratory development, and advanced technology demonstrations. To accomplish this, GACIAC's functions are to:

1. Develop a machine-readable bibliographic data base -- currently containing over 42,000 entries;
2. Collect, review, and store pertinent documents in its field of interest -- the library contains over 15,000 reports;
3. Analyze, appraise, and summarize information and data on selected subjects;
4. Disseminate information through the GACIAC Bulletin, bibliographies, state-of-art summaries, technology assessments, handbooks, special reports, and conferences;
5. Respond to technical inquiries related to weapon guidance and control; and
6. Provide technical and administrative support to the Joint Service Guidance and Control Committee (JSGCC).

The products and services of GACIAC are available to qualified industrial users through a subscription plan or individual sales. Government personnel are eligible for products and services under block funding provided by the Army, Navy, Air Force and DARPA. A written request on government stationery is required to receive all the products as a government subscriber.

Further information regarding GACIAC services, products, participation plan, or additional copies of this special report may be obtained by writing or calling: GACIAC, IIT Research Institute, 10 West 35th Street, Chicago, Illinois 60616-3799, Area code 312, 567-4519 or 567-4526; Fax 312, 567-4889.