

Navy Air Defense and Related Threat Simulation Validation Program

Navy Threat / Simulation Validation Coordinator
Code 53C000D, NAWCWD China Lake

Definition and Purpose

- ◆ “To determine the degree to which a simulator/target/model or simulation is an accurate representation of the threat from the perspective of its *intended use*.”

The Navy's "Air Defense and Related Threat Simulation Validation Program" Provides...

- ◆ **Customers such as OPNAV, NAVAIR and COMOPTEVFOR with....**
 - Validated threat systems & simulations to support DT&E, OT&E testing and Fleet training.
 - Validated systems to support accreditation.
 - Navy validation program management and oversight.

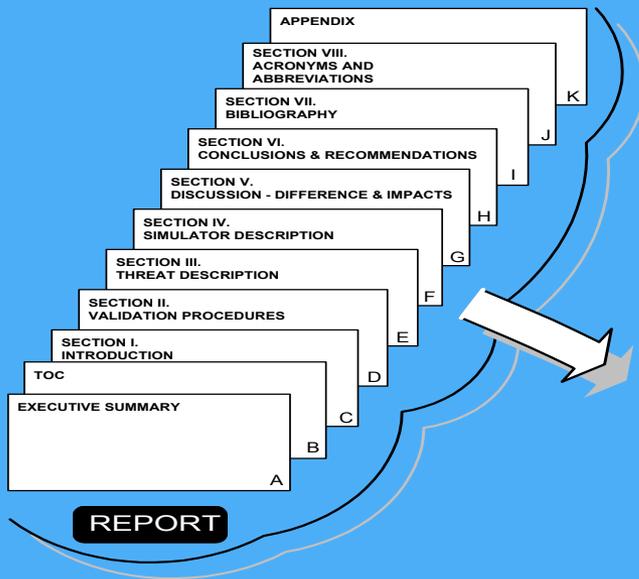
Compliances

- ◆ DOD 5000 Series Docs
- ◆ DOD Threat Simulation Program Plan TSPP, Annex I
- ◆ DOD Threat Definition Documents under Annex I in Appendix A through L
- ◆ DOD Threat Simulator Program Guidelines
- ◆ SECNAV 5200 Series Docs
- ◆ COMOPTEVFOR 5000.1

Type Systems Validated

- ◆ Actual threat hardware
- ◆ OAR Emitter/Receiver/Processor (ERP)
- ◆ OAR Emitters
- ◆ Hardware-in-the-Loop Simulations (HLS)
- ◆ Digital Missile Fly-out Simulations
- ◆ EO/IR and UV Systems
- ◆ C3, Surrogates, Jammers....

Validation Report Structure



| EXECUTIVE SUMMARY |
|---|
| ALL PERTINENT INFORMATION NO EXTRANEIOUS INFORMATION STANDALONE SECTIONS 1 THROUGH 6 TWO TO THREE PAGES |

| TOC |
|---|
| SECTION PARAGRAPH FIGURES TABLES |

| INTRODUCTION |
|--|
| WHAT THREAT SIMULATION REPRESENTS INCLUSION LIST EXCLUSION LIST WHAT VARIANTS PURPOSE/OBJECTIVE P.O.C |

| VALIDATION PROCEDURES |
|--|
| DIRECTIVES USED SOURCES OF DATA PROCESSES USED |

| THREAT DESCRIPTION |
|--|
| AS CURRENTLY DEFINED INCLUDED DIA APPROVED SOURCES OF THREAT DATA BLOCK DIAG OPERATIONAL DOCTRINE |

| SIMULATOR DESCRIPTION |
|--|
| INCLUDED FUNCTIONS 1. 2. EXCLUDED FUNCTIONS PROGRAMMABILITY DISCUSSION SPECIAL MODES 1. 2. |

| DIFFERENCES & IMPACTS |
|---|
| MOST IMPORTANT IMPACTS DIFFERENCES GENERAL ASSESSMENTS |

| CONCLUSION & RECOMMENDATIONS |
|--|
| OVERALL CONCLUSIONS 1. 2. RECOMMENDATIONS 1. 2. |

| BIBLIOGRAPHY |
|--|
| LISTED REFERENCED IN DOCUMENT UP-TO-DATE |

Tailored Threat Database - Appendix

| APPENDIX A1 |
|---|
| KEY TO ACRONYMS ABBREVIATIONS SCRIPTION |

| APPENDIX A2 |
|--|
| THREAT AND SIMULATOR DATA RANGE OF PROGRAMMABILITY VALIDATOR'S NOTES ANALYST'S COMMENTS |

| Threat Systems Office Number | Subsystem Parameter | Units | DIA EST. | Conf. Level | SIM Data | Diff./ *TSCP |
|---------------------------------|------------------------|-------|-------------|----------------|-------------|-----------------|
| R4117.01 | Transmitter Power | WATTS | 1KW | 2 | 600 | *400 |
| R4117.02 | | | | | | |

NAVY
VALIDATION
REPORT

Validation Process

DATA COLLECTION



THREAT DATA

- DIA-APPROVED THREAT DOCUMENTS
- CURRENT EWIR LISTING
- S&TI CENTER FME / OEM DOCUMENTS
- CONFIDENCE LEVELS ASSIGNED BY LEAD S&TI CENTER ANALYST



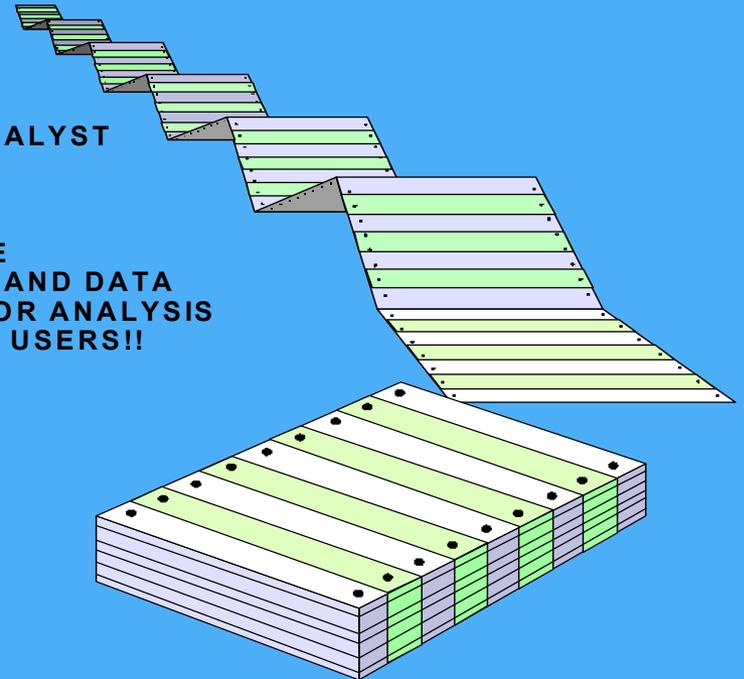
T&E AND TRAINING REQUIREMENTS

- TEST AND EVALUATION MASTER PLAN (TEMP) IS A SOURCE
- TECHNICAL INTERVIEWS PROVIDED ECM UNDERSTANDING AND DATA
- POTENTIAL T&E AND TRAINING ISSUES FORM THE BASIS FOR ANALYSIS
- SPECIFIC REQUIREMENTS ARE TO BE DETERMINED BY THE USERS!!



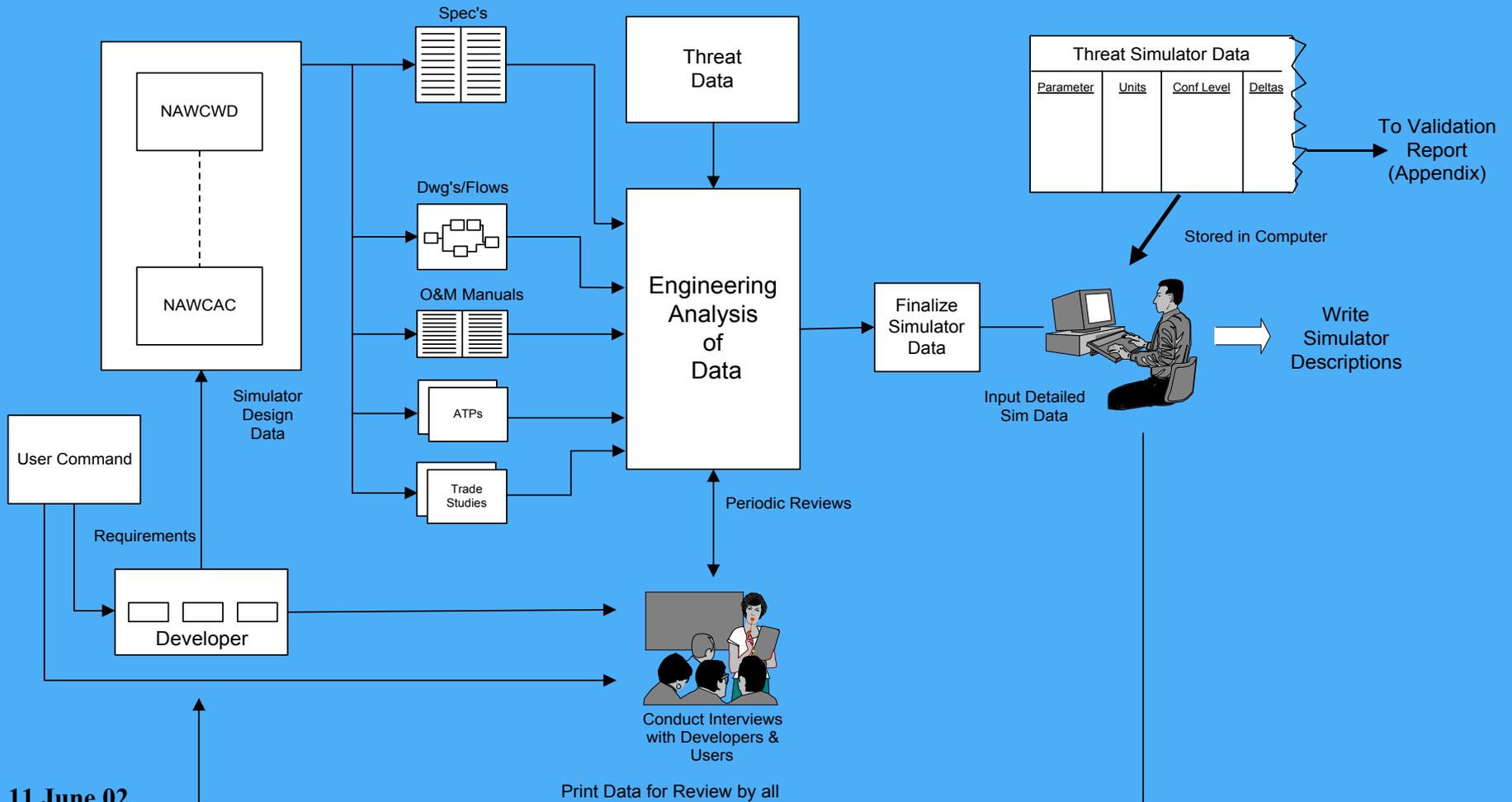
SIMULATOR DATA

- DESIGN SPECIFICATION DATA
- CDR DATA
- FACTORY / SITE ACCEPTANCE TEST DATA
- TECHNICAL INTERVIEWS WITH DEVELOPERS
- COLLECTION EMPHASIS ON CRITICAL PARAMETERS

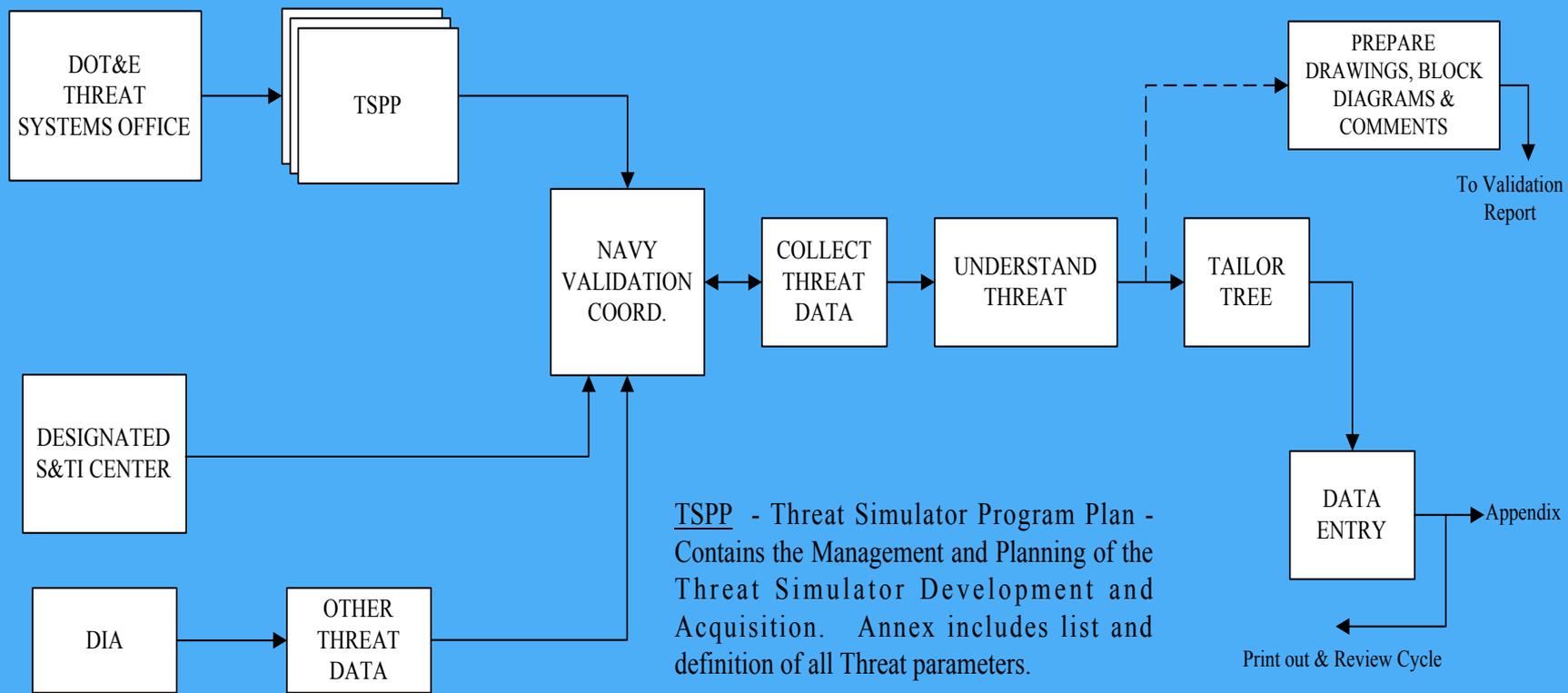


Simulator Data Collection

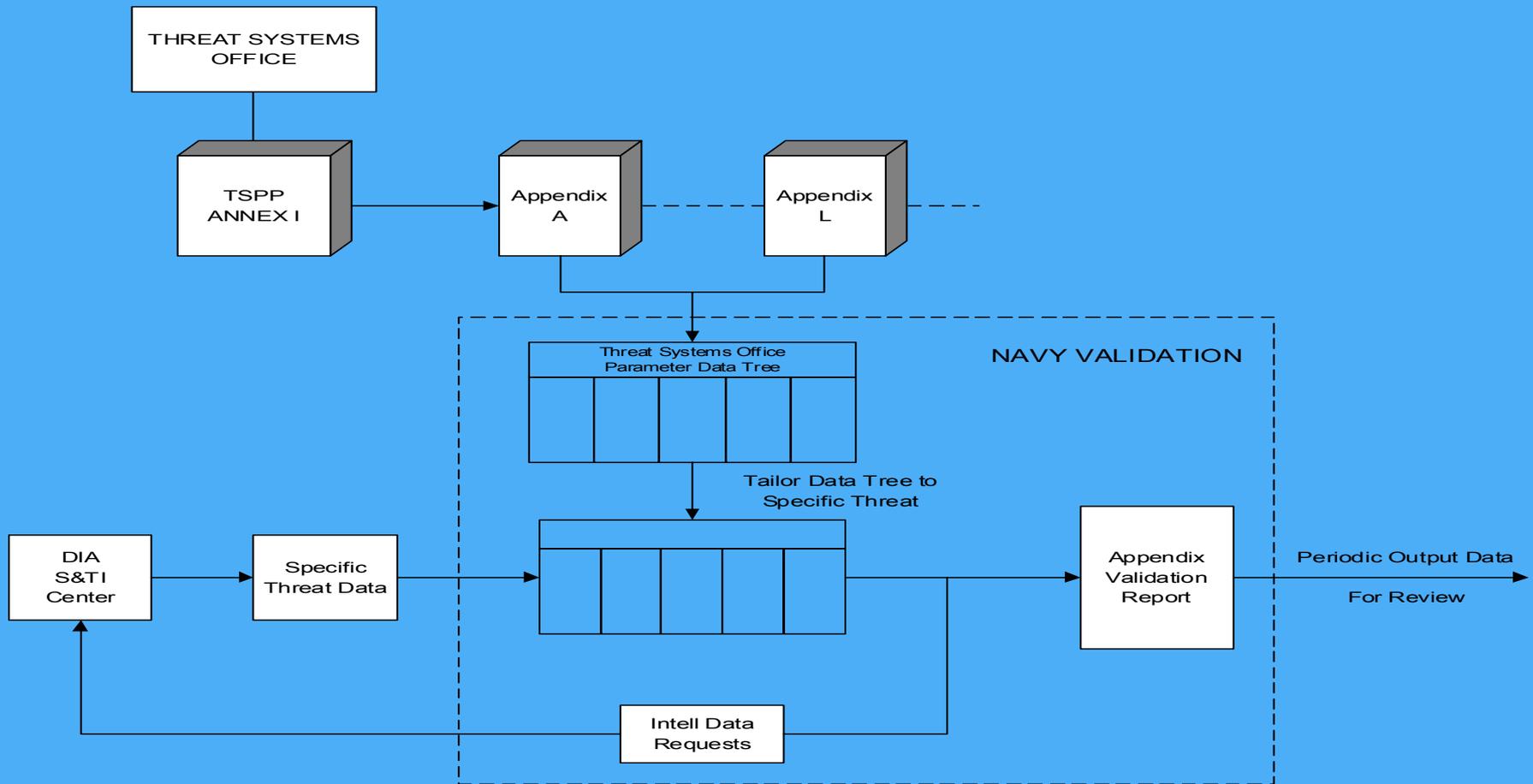
Simulator Data



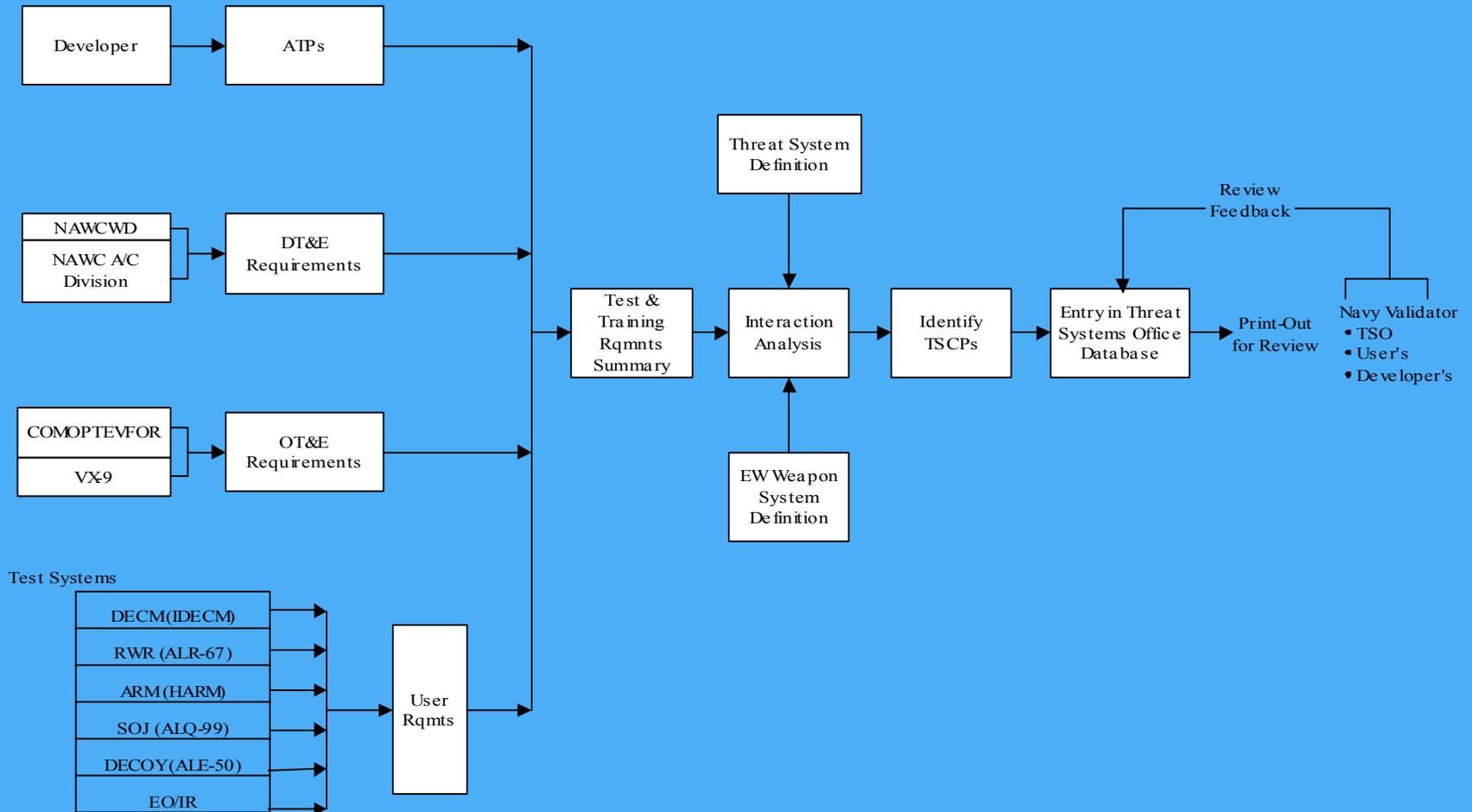
Threat Data Collection Process



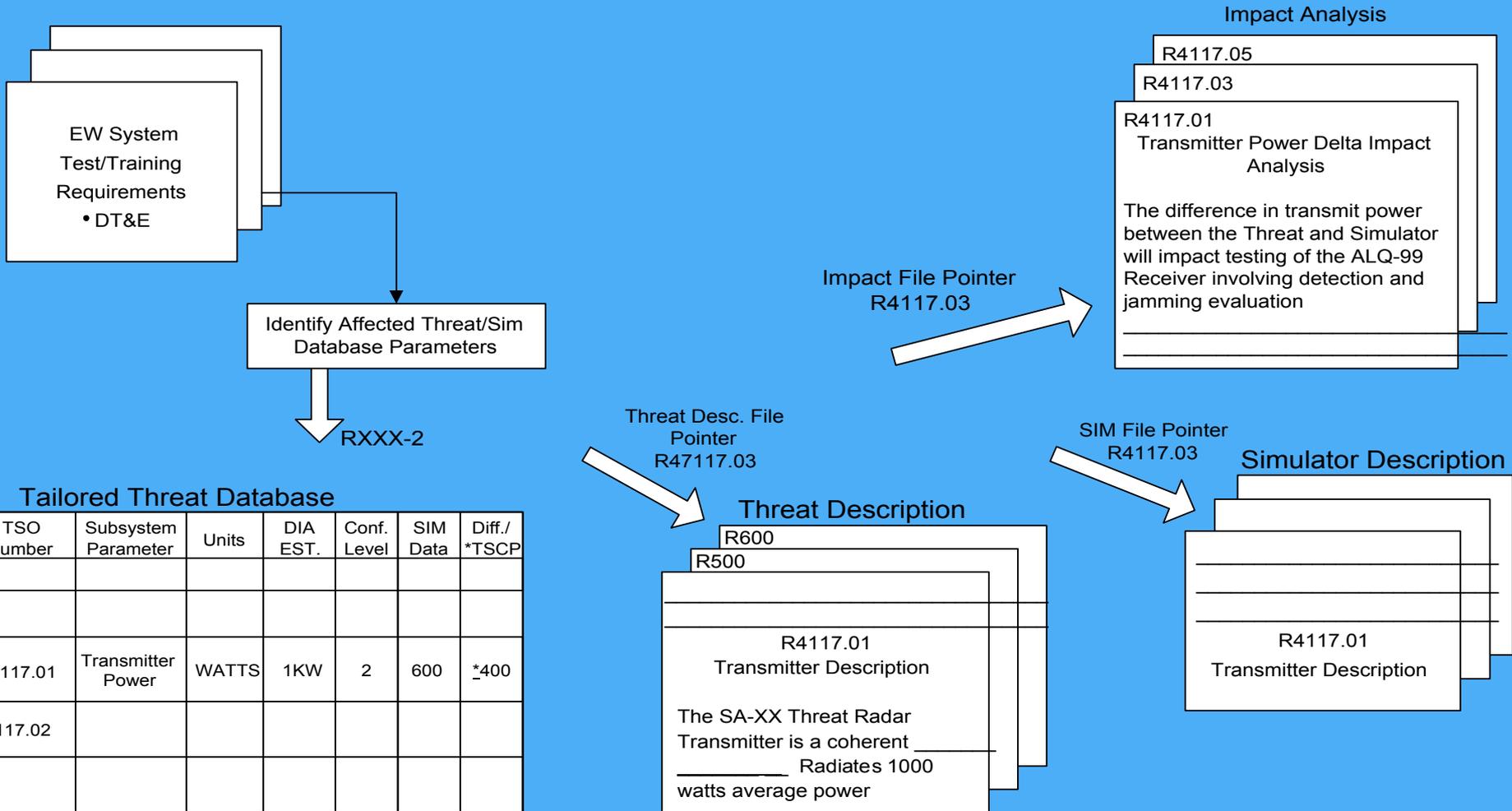
TDD Parameter Tailoring Process



Performance Parameters & TSCP Identification



Validation Database



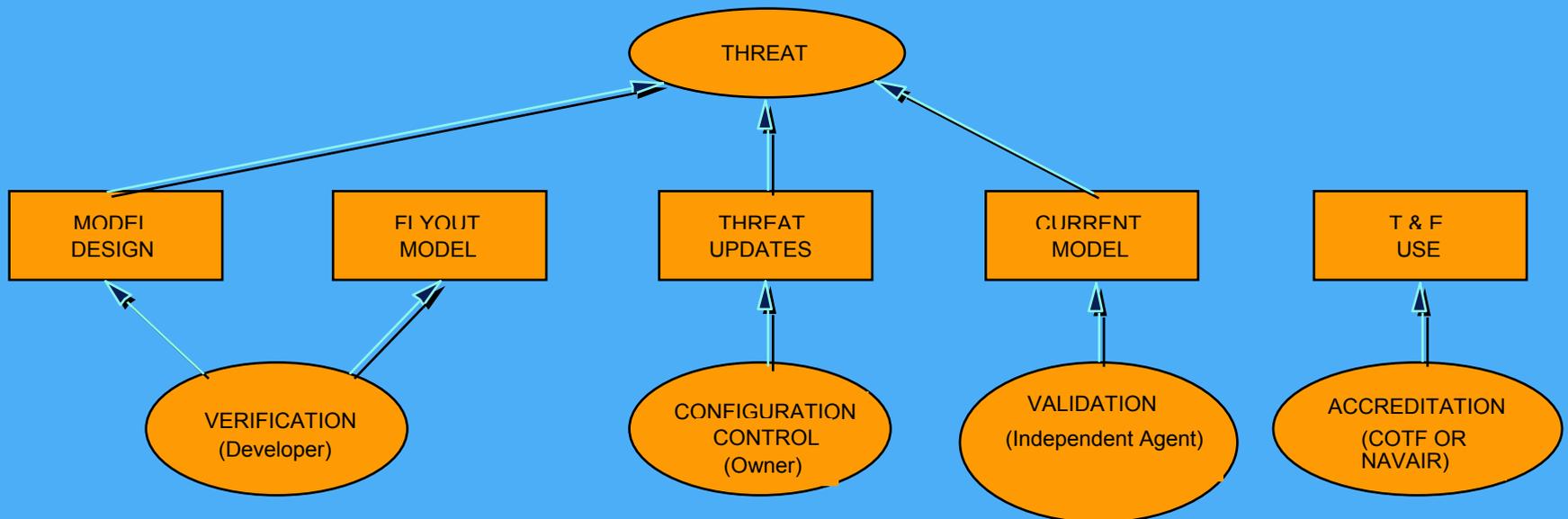
NAVY VALIDATION REPORT FORMAT

| Threat TDD NUMBER | SUBSYSTEM/PARAMETER | UNITS | DIA THREAT ESTIMATE | CONFIDENCE LEVEL/ REFERENCES | SIMULATOR DATA | DIFFERENCE/ *TSCPs |
|-------------------|---------------------------------|-----------|---------------------|------------------------------|----------------|--------------------|
| R3371.00 | ANTENNA ECCM | YES/NO | YES | 3 | NO | YES |
| R3371.01 | POLARIZATION ECCM | YES/NO | NO | 2 | NO | 0 |
| R337.02 | SIDELOBE BLANKING | YES/NO | NO | 4 | NO | 0 |
| R337.03 | SIDELOBE CANCELLER | YES/NO | NO | 4 | NO | 0 |
| R3371.00 | DIVERSITY TECHNIQUES | YES/NO | YES | 3 | YES | 0 |
| R33711.00 | ANGLE SCAN DIVERSITY | YES/NO | NO | 4 | NO | 0 |
| R33712.00 | SPATIAL DIVERSITY | YES/NO | NO | 4 | NO | 0 |
| R3372.00 | MONOPULSE | YES/NO | NO | 4 | NO | 0 |
| R4.00 | TRANSMITTER | YES/NO | YES | 1 | YES | 0 |
| R41.00 | PULSED FREQ | YES/NO | YES | 2 | YES | 0 |
| R411.00 | GENERAL | YES/NO | YES | 1 | YES | 0 |
| R411.01 | NBR OF TRANSMITTERS | INTEGER | 1 | 1 | 1 | 0 |
| R411.02 | TRANSMITTER TYPE | TEXT | MOPA(CFA/TWT) | 1 | MOPA(CFA/TWT) | 0 |
| R411.03 | TRANS BLOCK DIAGRAM, PULSED | FIGURE | SEE TEXT | 3 | SEE TEXT | |
| R4111.00 | SIMULTANEOUS/MULTIPLE RFS | YES/NO | YES | 1 | YES | *0 |
| R4111.01 | NBR OF SIMULTANEOUS RFS | INTEGER | 2 | 2 | 2 | 0 |
| R4111.02 | SIMULTANEOUS RF SEPARATION | MEGAHERTZ | 125 | 2 | 125 | 0 |
| R4111.03 | TIME DELAY BTWN RFS | MICROSEC | 4.5 | 2 | 3.0 TO 6.5 | 1.5 TO 2 |
| R4112.00 | PULSED RF CONSTANT | YES/NO | YES | 2 | YES | *0 |
| R4112.01 | RF LIMITS | GIGAHERTZ | 2.12 TO 2.37 | 2 | 2.1 TO 2.425 | 0.02/0.0555 |
| R4113.00 | RF CHANNELIZATION | YES/NO | YES | 1 | YES | 0 |
| R4113.01 | NBR OF CHANNELS | INTEGER | 8 | 1 | 80 | 72 |
| R4113.02 | CENTER TO CENTER RF SEPARATION | MEGAHERTZ | 9 TO 15 | 2 | 2.5 | YES |
| R4113.04 | AVAIL PER SYSTEM | INTEGER | 8 | 2 | 80 | 72 |
| R4114.00 | LIMITED FREQ CHANGE CAPABILITY | YES/NO | YES | 4 | YES | *0 |
| R41141.00 | DISCRETE LIMITED FREQ CHANGE | YES/NO | YES | 1 | YES | 0 |
| R41141.01 | DISCRETE LIMITED FREQ CHANGE | YES/NO | YES | 1 | YES | 0 |
| R41141.03 | NBR OF RFS | INTEGER | 16(8PAIRS) | 1 | 160 | 144 |
| R41142.00 | CONTINUOUS LIMITED FREQ CHANGE | YES/NO | NO | 3 | NO | 0 |
| R4115.00 | SMALL INTENTIONAL RF VARIATIONS | YES/NO | NO | 3 | NO | 0 |
| R4116.00 | PULSED RF AGILITY | YES/NO | YES | 2 | YES | *0 |

NAVY MODEL VALIDATION

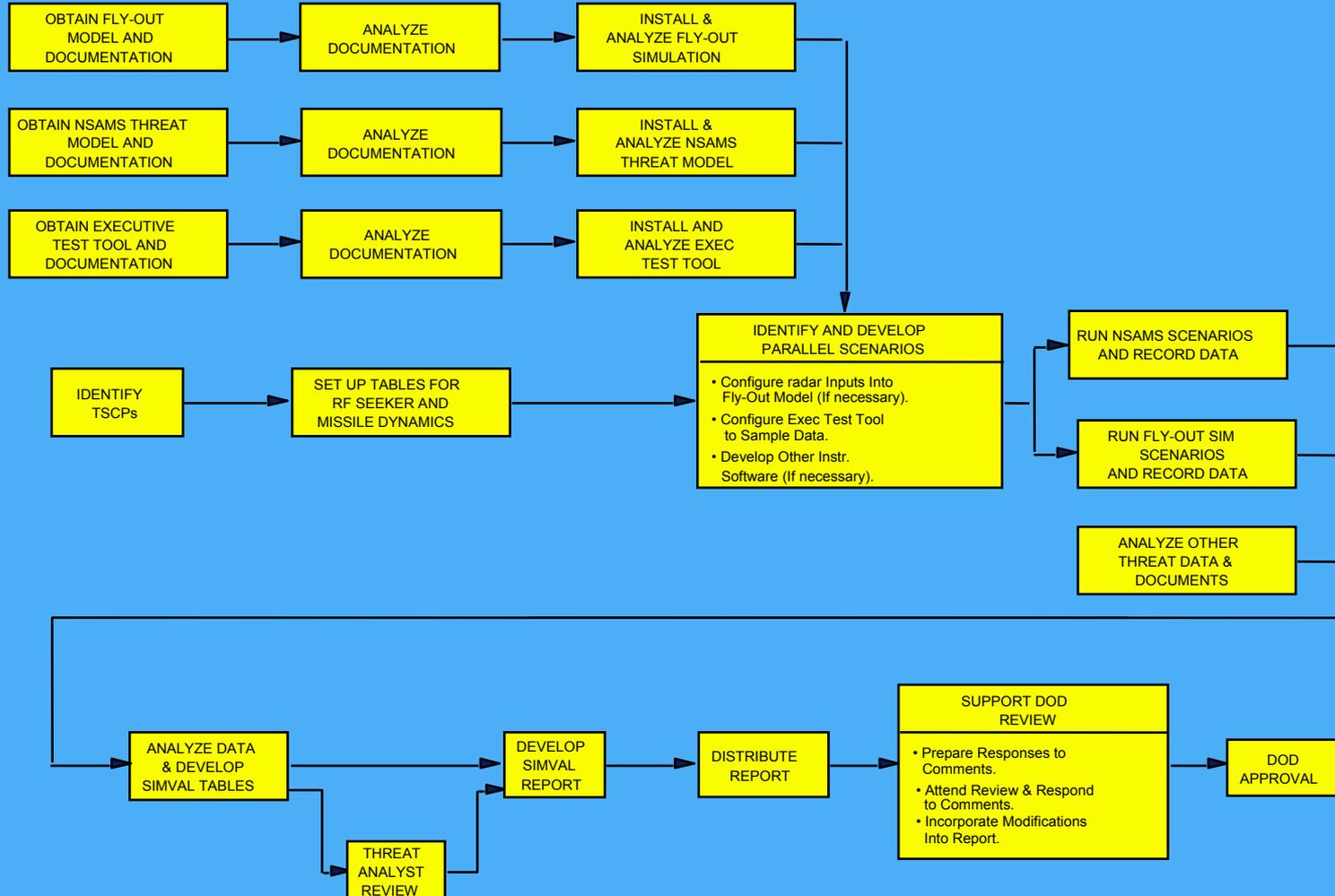


MODEL MANAGEMENT
(Developer or PM)



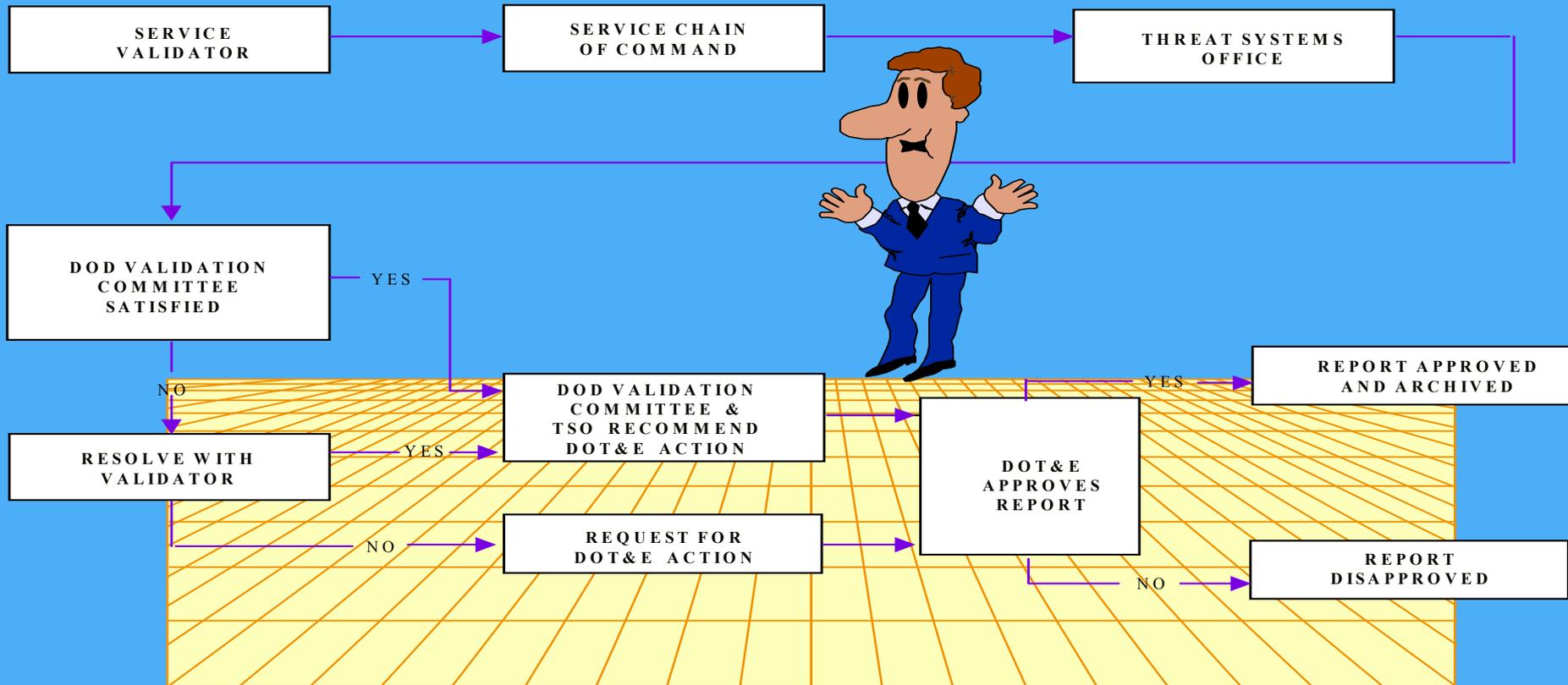
NAVY MODEL VALIDATION

FLY-OUT SIMULATION VALIDATION PROCESS



Approval Process

REPORT APPROVAL



Summary

- ◆ Navy funded Air Defense and Related test assets used in support of milestone decisions are being successfully validated under this program.
- ◆ “54” Navy Validations have received DOD approval.
- ◆ Validations are being conducted in accordance with DOD, DOT&E, SECNAV, OPNAV, and COMOPTEVFOR guidelines, procedures and instructions.

Questions??

?

Easy 17 Step Process Cont.

- ◆ **1. Begin planning. Identify requirements for the intended uses of the Model, Simulator, Simulation or Actual Threat Weapons System.**
- ◆ **2. Identify the representative threat ELINT Notation (ELNOT), or ELNOTs, associated with the threat data the system is to be validated and compared against.**
- ◆ **3. Download and print the ELNOT or threat data file from the current version of the Electronic Warfare Integrated Reprogrammable (EWIR) CD-ROM or applicable data base and software media.**
- ◆ **4. Become familiar with the threat data contents of the file, and review the listed DIA or cognizant Intel Center approved threat reference documents listed at the end of the data section to determine the availability of exploitations and other related threat definition documents.**
- ◆ **5. Convert the EWIR or applicable data base file to the DOD Threat Definition Document (TDD) parameter number format using the available software program. Tailor the TDD parameter tree to match the threat system configuration as your baseline to compare against. If this is a model being validated conversion of performance parameters, mass, flight profiles, trajectories, plots and flight profiles, acceleration curves, ... etc. will be included in this important step.**

Easy 17 Step Process Cont.

- ◆ 6. Write the Table of Contents, Introduction and Validation Procedures sections.
- ◆ 7. Obtain additional threat definition documents or data from the EWIR or the applicable data base references or other known sources, i.e., OEM-, FME-type documents. Obtain NSAMS or threat model.
- ◆ 8. Write the Section III (Threat Description) for the validation report using the EWIR or applicable data base file and other DIA or cognizant Intel Center approved documents. A thorough, comprehensive understanding of the threat system is important for the accurate validation of any model or simulation.
- ◆ 9. Complete the threat data entries in the Standard Validation Criteria (SVC) tables for the appendix A-2 parameters and performance data section of the report using all available source data. Add the TSO branch head parameter numbers for the branches that are not included in the EWIR data.

Easy 17 Step Process Cont.

- ◆ 10. Request, obtain, collect all available Model and simulation data from the range, developer, model developer, contractors, and any others that might be involved. This Model and simulation data collection effort should be started concurrently with Item #2. Model and Simulation data can include specifications, integration plans, program review material (PDR, CDR, IPR), factory acceptance test results, acceptance test plans and results, block diagrams, site layouts, and equipment photographs, model runs, etc. Interviews with program managers, model developers and project engineers are extremely useful in understanding the model or simulation obtained
- ◆ 11. Write section IV (Simulation or Model Description) using all available collected data. During this description writing effort, and after obtaining a thorough understanding of the threat system from writing section III, some differences between the threat and the model or simulation will become apparent.
- ◆ 12. Complete the model or simulator data column in the SVC tables using all available model and simulation data.

Easy 17 Step Process Cont.

- ◆ **13. Review the planned, possible, and future test requirements for the model or simulation, as related to the designed or planned "intended use" of the system. Identify the possible "threat simulation critical parameters" (TSCP) or "model performance parameters" (MPP's) that could be associated with this new model or simulation when compared to its intended use and the type of test requirements that the model or simulation was designed to satisfy. Note the TSCPs or MPPs in the SVC tables for each associated parameter. Run the flyout model and run the NSAMS model. Note all differences.**
- ◆ **14. Calculate the parametric differences between threat data / model and the simulator, simulation / model being compared to. Complete the differences column in the appendix tables. Document all differences.**
- ◆ **15. Identify all of the noted differences between threat system and simulator. Write section V (Differences and Impacts) of the validation report. Discuss the possible impact of the noted differences while applying past experiences and knowledge of the countermeasures systems, known test requirements, and test range capabilities and limitations. Some differences can be significant while other would have no impact on testing.**

Easy 17 Step Process Cont.

- ◆ **16. Write section VI (Conclusions and recommendations) briefly outlining the findings.**
- ◆ **17. Write the Executive Summary that contains a top-level overview of the entire report. No material is provided here that is not provided in the other six sections in greater detail. This section should be two to three pages in length, unless there are a very large number of differences and impacts to address. This should be a stand-alone section.**

REPORT FORMAT



Standard Validation Report Format

Executive Summary. This section is the last section written and is a condensed version of Sections I through VI. The major elements of the six sections should be covered. No material is provided here that is not provided in the other six sections in greater detail. Much of the detailed discussion is not included here, but is found only in the main body of the report. This section should be two to three pages in length, unless there are a very large number of differences and impacts to address. This should be a stand-alone section.

Section I, Introduction. This section should briefly state what threat this simulator is expected to represent, what portion of the threat is included, what is left out, and the relationship of this simulator to others if it is a portion of a larger system, or a modification of a larger system. It also should state whether the simulator is expected to represent multiple variants of the threat, if such variants exist. The purpose or objective of the validation report should be stated. This section should include a statement that the validation report describes the status of the simulator's ability to emulate the threat at that point in time, and that there may have been changes in the threat definition or in the simulator since the validation report was written. The introduction should identify a point of contact for users to gain additional information.

Standard Report Format Cont.

Section II, Validation Procedures. This section should identify the directives that apply to this report. It should identify the sources of data for both the threat and the simulator, along with the process of determining the impacts of the differences between the threat and the simulator that have been documented.

Section III, Threat Description. This section should provide a brief (3-10 pages) narrative description of the threat as it is currently defined. The section should also state that the data has been extracted from DIA documents or should identify the other documents used as source data for the threat information. State if the DIA has approved any or all of the data that was drawn from non-DIA documents. Generally, block diagrams should be placed in this section. Operational doctrine, time to sequence from acquisition to track to launch to intercept, type of system, etc., are appropriate in this section. Discussion that builds on the data provided in Appendix A, or provides additional explanation of the information in Appendix A, should be included.

Standard Report Format Cont.

Section IV, Simulator Description. This section should specifically identify all functions of the threat that are included, and any of the functions of the threat system that are not included, as part of the simulation. If some portions are simulated in hardware, for example, target tracker and missile seeker, while other portions are simulated in software, for example, missile fly-out, that too should be stated. It is preferred that a simulator system be fully addressed in one report, rather than breaking it apart into two or more reports, (for example, the target tracker in one report with the missile seeker and fly-out model in a separate report). In many cases the simulator is programmable in a number of areas and could be readily changed as the threat definition changes. Significant programmability should be covered in this section. If programmable features cover the current threat estimate, the report should include this information. If there are any special modes of operation, they should be described here.

Standard Report Format Cont.

Section V, Discussion of Differences and Impacts. This section is the most important of the validation report. With the data in Appendix A, this is the real meat of the report. This section should address all significant impacts on testing or training that may occur due to differences between the current threat and the simulator. These statements of impacts may be based on a significant difference between the threat and the simulator, or they could be based upon a group of differences. If there are differences, which tend to counter-balance the impact each may have individually, they should be discussed together. Do not address each difference of the threat and the simulator, only those which individually or collectively could be expected to impact test or training results. While specific systems that have been designated to be tested against the simulator can be useful in identifying some of the impacts of differences, the validators should consider all types of systems that may undergo testing with the simulator when identifying the impacts of differences.

Standard Report Format Cont.

Section VI, Conclusions and Recommendations. This section should address the overall conclusions and recommendations that can be reached on the basis of the impacts of the differences between the current threat and the simulator. Several significant impacts may affect only one type of test, leaving the simulator well suited for other tests; this should be stated. In some cases, the simulator may be so different from the threat in several different areas that a modification is recommended.

Section VII. References. This section should list all references used in the report.

APPENDIX A. Standard Validation Criteria Data

Section A1. This section should provide a key to the abbreviations used in the data entries in Section A2. All items, such as NA or N/A, NAp, NSm, should be explained. Whenever threat data has no confidence level associated with it, the report should state how the data in the Confidence Level column has been coded to show that fact.

Standard Report Format Cont.

Section A2. This section should contain the SVC from the appropriate Threat Simulator Program Plan Annex I Appendices, with all threat and simulator data. In cases where the simulator has been made programmable, do not simply state programmable. The range of programmability must be stated along with the fact that the function is programmable. If any of the programmable items have been programmed such that they do not match the current threat definition, this also must be stated. Validators' notes and threat analysts' comments should be identified in the Notes/References column and included at the end of the section. All portions of the SVC should be addressed; however for those portions which do not apply, such as Continuous Wave parameters for a pulsed radar system, simply state "_____ Applicable" as the header entry for that group of parameters. Delete subordinate parameter numbers and names in the group from the report. The threat analyst should already have done this. Do not leave out a portion of the SVC without some explanation.