

Threat Representation – Guidance

Guidance

Threat systems, tactics, and overall capabilities must be adequately represented in operational testing to yield credible, valid results of a system's performance in a realistic operational environment. Information and guidance for characterizing threat systems, tactics, and overall capabilities is provided by the Defense Intelligence Agency (DIA), the Service intelligence production centers, and other intelligence agency reporting. To obtain the additional threat system intelligence that is necessary for test planning, but which is beyond the level of detail captured in the System Threat Assessment Reports (STARS), test planners should consult related intelligence documentation such as Integrated Technical Evaluation and Analysis of Multiple Sources (ITEAMS) reports and Joint Country Operating Force Assessments (JCOFA). To obtain information on the missions and targets of greatest interest to the system under test, and for operational context, planners should consult system employment documents such as field manuals, concepts of employment, analyses of alternatives, and operational mission summary/mission profile documentation.

Emphasis should be placed on adequate representation of threats, threat attributes, and threat environments that are most relevant to the evaluation of the system under test, including evaluation of system lethality and survivability.

The TEMP should illustrate that threats will be adequately represented in testing by including plans to:

- Section 1.3.4. System Threat Assessment: Identify the threats and threat attributes of most interest to the evaluation of the system under test. Review intelligence community assessments and reports to determine the threats the system is likely to face in the operational timeframe(s) and theaters of interest. Perform a preliminary appraisal of threats and threat attributes that are likely to have the greatest impacts on operational effectiveness. Consultation with technical and tactical subject matter experts may be required. ([Example](#))
- Section 1.3.6. Special Test or Certification Requirements: The threat assessment may reveal that critical threats, targets, or threat attributes are not available to support operational or live fire testing. The TEMP should describe the need for development of special threat or target systems and any activities necessary to validate these systems for use in testing. ([Example](#))
- Section 3.5. Operational Evaluation Approach: Summarize the operational test events, key threat simulators and/or simulation(s) and targets to be employed, and the type of representative personnel who will operate and maintain the system. ([Example](#))
- Section 3.5.4. Operational Test Limitations: Identify projected critical/severe or major test limitations stemming from inadequate threat representation, and plans to mitigate those limitations. ([Example](#))

Threat Representation – Guidance

- Section 4.2.5 and Section 4.2.6. Threat and Target Resources: Identify the necessary quantity (numbers of troops, attack aircraft, surface-to-air missiles, torpedoes, tanks, etc.) of threat systems or threat surrogates necessary for all test events. Specify responsibilities, timeframe and resources required to complete validation of threat surrogates. Include threat targets for LFT&E lethality testing and threat munitions for vulnerability testing. ([Example](#))

Each Service is responsible to conduct technical and operational comparisons (validation) between the actual threat attributes and the attributes of planned threat systems (actual or surrogate) for operational or live fire testing. Validation activities should be planned, budgeted, and scheduled to complete well in advance of operational or live fire testing.

DOT&E monitors the validation and approves – through the test plan – the use of all threats and threat surrogates for operational and live fire testing.

References

[Defense Acquisition Guidebook, Chapter 9](#)