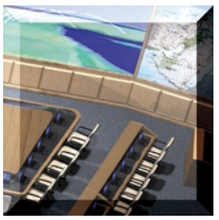

Laying the Foundation for Successful Systems Engineering

Fred R. Skolnick and Phillip G. Wilkins

The end of the Cold War has forced the Navy to develop new cost-effective systems that must be flexible and sufficiently robust to successfully conduct a host of worldwide missions. These missions increasingly require operations in littoral regions, a complex arena characterized by a multitude of potential threats, reduced maneuver areas and reaction times, and stressing physical environments. The Design Reference Mission (DRM) defines the projected threat and operating environment baseline for a rigorous systems engineering process to help ensure that future Navy systems can meet 21st century challenges and uncertainties. The DRM defines the problem, not the solution, via families of specific operationally representative situations and supporting threat and physical environment characterizations. This article discusses the need for and role of the DRM in the Navy systems engineering process, examines the mission's objective, and traces the recent evolution of the DRM concept. (Keywords: Design Reference Mission, Operating environment, Scenario, Systems engineering, Threat characteristics.)

INTRODUCTION

As we enter the new century, the end of the Cold War and other "sea changes" in the worldwide geopolitical situation have dictated fundamental shifts in the Navy's roles and missions, spawning new demands on weapon systems. Today's Navy force structure and weapons, much like those of its sister services, were developed to counter a formidable, yet relatively well-understood adversary, the Soviet Union. The sudden demise of the Soviet Union has created a multipolar threat environment in which uncertainty abounds: Who are our probable adversaries? What is the potential battle space?

Trying to predict where, when, and how a conflict may arise becomes even more difficult. This degree of uncertainty requires forces and systems that can successfully conduct a wide spectrum of operations in a variety of physical environments against adversaries having a range of military capabilities. In addition, with Navy operations becoming an integral element of a Joint force, a significant requirement emerges to develop and evolve a naval warfighting capability that is highly effective and a critical contributor to Joint force success. The creative use of existing resources, significant modifications to these resources, and new designs are needed to maintain an effective naval force. The challenge is to provide flexible, robust, yet cost-effective solutions.

The Need

A common, authoritative threat and operating environment baseline is critical to efficient and successful systems engineering. In the past, the threat, environment, and operational scenarios used for systems engineering analysis were largely system-specific and defined by individual programs or industry. For stand-alone systems, this practice may be acceptable; however, for interoperable systems destined to be integrated into a "system of systems," this approach can make comparison of design alternatives difficult or technically invalid. The Design Reference Mission (DRM) seeks to provide a common framework to link systems engineering efforts and help ensure an "apples-to-apples" comparison of analytical results.

The evolving DoD systems acquisition process heightens the need for the strong threat and operating baseline provided by the DRM. The traditional acquisition process, i.e., one in which a government team develops detailed system specifications that are then provided to industry to guide system development, has been modified to involve industry earlier in the process. Industry now functions as an integral member of the systems engineering team or may even replace the government in the development of system concepts and specifications. Figure 1 illustrates the Common Systems Engineering Process initiated for the Navy Theater-Wide (NTW) Theater Ballistic Missile Defense (TBMD) and other programs under Program Executive Office Combat Surface Combatants (PEO (TSC)) sponsorship. This process is consistent with guidance identified in the Electronic Industries Association's *Interim Standard on Systems Engineering*.[1] As seen in Fig. 1, the DRM is as a key element of the system operating environment definition (step 1), which establishes the foundation for engineering trade studies and specification development. For the NTW Program, a government/industry systems engineering team conducted steps 2 through 5 and provided feedback that was used to refine the DRM.

Acquisition reform initiatives that shift the detailed engineering trade-off analyses, concept evaluation, and development of system-level performance specifications to the Navy's industry partners have a profound impact

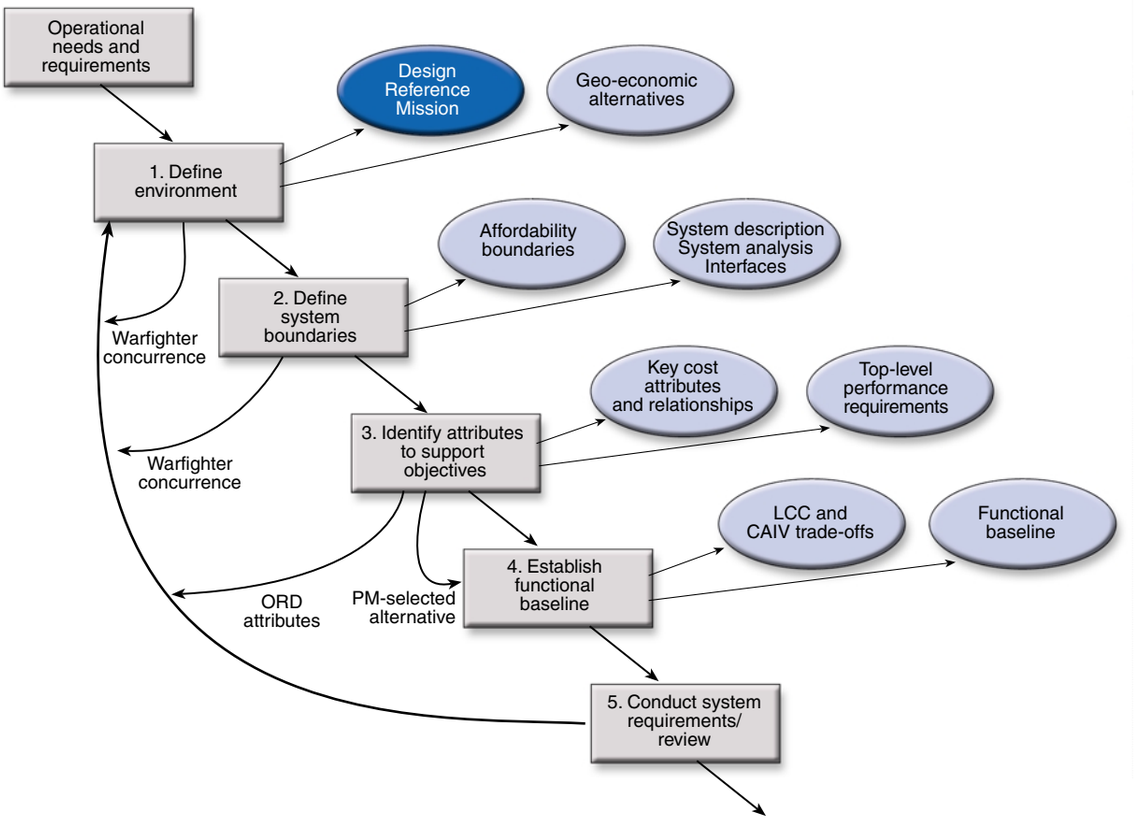

Figure 1. Common Systems Engineering Process. Note that the process elements are partially concurrent, nonsequential, and iterative. On the basis of feedback from program managers (PMs), operators, and others, the process is revised or refocused as needed. The products of the process are shown in the ovals. (CAIV = cost as an independent variable, LCC = life-cycle costs, ORD = Operational Requirements Document.)

on the Navy's role in the development of its own systems. In this new process, as implemented for the 21st Century Destroyer Program, the Navy provides an official procurement information package to perspective development contractors. The package includes a top-level statement of its requirements and a description of the naval forces and operations that will use the proposed system. Based on this information, industry proposes various solutions, with more detailed system requirements, and ultimately system specifications.

The new approach mirrors current business practices that minimize specific direction and enable workers (or in this case, industry) to propose innovative, efficient solutions while reducing the involvement of management. Although the potential benefits are significant, the associated risks are also increased. One fundamental risk is that industry's solution, however elegant or efficient, may solve the wrong problem. Since active government participation in the process shown in Fig. 1 effectively ends after step 1, the problem definition is frozen much earlier in the process. Thus, it becomes imperative for the Navy to carefully and comprehensively define the problem, both in terms of the missions it needs accomplished and the environment in which proposed solutions must perform. Although more traditional defense acquisition processes also require this same clear definition of mission needs and operational environments, they typically offer more opportunity to adjust and refine the operational context description as concepts are developed and performance specifications are defined.

A common baseline is fundamental to understanding and evaluating the complex problem of how a new system will function as a member of a team comprising other Navy, Joint, coalition, or even nonmilitary participants. Several initiatives are ongoing to exploit the synergy of viewing individual ships (or systems), existing or new, as part of a larger system of systems. Thus a multimission surface combatant would be connected with other nodes (ships, naval aviation, national and Joint service systems, etc.) via automated systems such as the Cooperative Engagement Capability, Joint Tactical Information Distribution System, and Global Command and Control System-Maritime. A ship, along with its systems and subsystems, will therefore serve as an integral element of a battle force.

Although implementation of this approach should improve the military effectiveness of existing systems, modifications and new systems will still be required to fill performance shortfalls and replace obsolete systems. Multimission and interoperability requirements complicate the system development process, particularly within the current, often "stovepiped," single-mission or single-platform focus.

For the foreseeable future, new major systems will need to demonstrate that they are sufficiently robust, militarily effective, and operationally relevant in their projected threat and operational environments. The successful development of tomorrow's ships and combat systems demands a rigorous systems engineering process built on a comprehensive understanding of the projected threat, the physical environment, and the increasingly complex "Blue Force" system of systems, which collectively define the ships'/systems' anticipated operating environment.

The Objective

The DRM concept seeks to define the problem, not the solution. Its primary objective is to characterize the threat and operating environment that will serve as the baseline to support systems engineering activities, i.e., requirements definition/refinement, concept development/evaluation, trade study analysis, design, test and evaluation, etc. This objective is common across the variety of system acquisition policies used by the Navy. Under acquisition reform, the operational requirements and DRM provide the only definition of requirements and operational employment to industry for system development. As shown in Fig. 1 for the government-led development process, the DRM feeds the development and certification of a system functional baseline and provides support through the entire life of the program. Thus the DRM must support the program throughout the systems engineering process. It is important to note that feedback from program managers, operators, and other DRM users helps to ensure that the final iteration of the DRM will provide the best, most relevant support possible. Although it does not contain economic information per se, the DRM baseline may give indirect support to a variety of cost analyses, including life-cycle cost and cost-as-an-independent-variable trade-off studies.

EVOLUTION OF THE DRM

The DRM is not an entirely new concept and can trace its lineage at least back to the mid-1960s when requirements for well-defined functional and environmental mission profiles, and later a threat baseline, were identified. Built upon earlier efforts that include elements of the *Aegis Threat Handbook* initiated in the early 1970s, the current DRM concept differs significantly from prior efforts in that the processes and products have been tailored to more effectively meet user requirements and to support today's systems engineering process.

A DRM for Theater Air and Missile Defense (TAMD) was initiated in early 1997 as part of a new common systems engineering process for the (then) PEO for Theater Air Defense (now PEO (TSC)). The TAMD DRM was envisioned as a set of products consisting of an overarching document supported by

annexes for the major TAMD mission areas: TBMD, Anti-Air Warfare (AAW), Overland Cruise Missile Defense (OCMD), and the Area Air Defense Commander (AADC). The TBMD Annex has since been split into the Navy Area TBMD (NATBMD) and NTW Annexes. The overarching document provides the common campaign context for the annexes as well as a specified methodology and any threat and environment data applicable to multiple annexes. The annexes contain mission-specific operational situations (OPSITs) and related threat and operating environment characterizations. As of this writing, other DRMs in various forms have been or are being developed for a range of programs including the 21st Century Destroyer (DD 21), new aircraft carrier (CVNX), Common Land Attack Warfare (LAW) System (CLAWS), vertical-launched unmanned aerial vehicle, and Battle Force Engineering Initiative.

DRM Profiles

In 1985, DoD published *Transition from Development to Production*,[2] which presented a series of critical-path templates to help program managers understand and reduce the risks involved with the design, test, production, and sustainment of increasingly complex weapon systems. These templates, commonly referred to as the Willoughby Templates (after W. J. Willoughby, Jr., Chairman of the 1982 Defense Science Board Task Force on this topic), also appeared in the Navy publication *Best Practices, How to Avoid Surprises in the World's Most Complicated Technical Process*[3] in 1986.

These publications identified the development of a DRM Profile (DRMP) as the first of 14 steps used to reduce risk in the design process. A DRMP comprises a Functional Mission Profile and an Environmental Mission Profile. The former shows all mission-related system functions on a timescale. Also on a timescale, the Environmental Mission Profile defines the envelope of environments for weapon system storage, maintenance, transportation, and operation. Based on these government-provided profiles, industry developed the *system* functional and environmental profiles that became the formal design requirements. NAVSO P-6071 lists the DRMP as a "Best Practice" and cites the following benefits to program managers[3]: design-to-specification correlates to actual use conditions, conservative design margins are established, equipment failures in the field are reduced, and system design meets all lifecycle functional and environmental criteria.

The DRMP has become a standard product within the reliability, maintainability, and availability (RMA) community, with profiles produced for major ship programs (DDG 51, CVNX, etc.). The RMA-focused DRMPs (sometimes called DRMs) are typically time lines of varying durations (months to years to decades) that list combat and noncombat activities without providing detailed descriptions of these activities.

The Handbooks

The current DRM shares more similarities with the *Littoral Warfare Handbook* (LWH) than the DRMP. The LWH began as the *Aegis Threat Handbook* mentioned earlier to address concern over the lack of a common, authoritative threat definition. The use of the *Aegis Threat Handbook* was mandated by the Aegis Program Manager for any system effectiveness evaluation being conducted in support of his program. As illustrated below, the focus of the handbook shifted in the post–Cold War era from the traditional emphasis on open ocean operations to a phased introduction of other mission areas like Anti-Submarine Warfare (ASW) and Naval Surface Fire Support (NSFS), etc., and threats such as Land Attack Cruise Missiles (LACMs), Mine Warfare (MIW), and surface ships (including small boats) associated with multimission surface combatant operations in the littorals.

- *Aegis Threat Handbook* (1971)
- *AAW Threat Handbook* (1976)
- *Surface Warfare Threat Handbook* (1982–1984)
  - Vol. 1A, Threat Summary
  - Vol. 1B, Environment
  - Vol. 1C, Battle Overview
  - Vol. 2A, AAW Threat
- *Littoral Warfare Handbook* (1994–2000)
  - First Edition (with emphasis on AAW)
  - Second Edition (added MIW, ships, LACMs)
  - Third Edition (adds ASW, NSFS)

The LWH presents a variety of warfare mission-specific engagement situations and multiwarfare operational scenarios that feature stressing threat and environmental conditions. Each scenario provides a brief description of a specific campaign context; collectively, the scenarios define the threat and operating environment for Aegis cruisers and destroyers. The LWH also includes detailed characterizations of the threat, background traffic, weather, and other factors required to assess system performance and overall platform effectiveness.

DRMP and LWH Limitations

Examination of the DRMP and LWH revealed shortfalls in their ability to support the full spectrum of systems engineering activities. Existing DRMPs provide far less fidelity than that required to conduct detailed engineering or force-level analysis. The RMA community's need for DRMP information, however, is acknowledged and addressed by the inclusion of a Mission

Profile within the DRM to document the full range of activity of major system elements over the prescribed campaign.

As already noted, the Aegis community has used the LWH successfully for many years to provide similar support as that envisioned for the DRM. As such, although not formally a DRM, the LWH can be viewed as the *de facto* DRM for Aegis cruisers and destroyers and has been used as the template for DRMs for other platforms. However, it does not offer the comprehensiveness and depth of detail in any specific warfare area that is needed for a strong, focused baseline to support the full range of systems engineering activities.

The best features of the DRMP and LWH were leveraged to create a DRM concept of families of mission- or platform-specific OPSITs linked by a common campaign that would support both system performance and RMA analysis. In addition, mission-specific OPSITs have the significantly more detailed associated threat characterizations required for engineering-level analyses.

THE DRM CONCEPT

The DRM defines the specific projected threat and operating environment baseline for a given force element, which may range from a single-purpose weapon system to a multimission platform to a multisystem, multiplatform system of systems. It is primarily an engineering/design tool to support systems engineering activities by identifying significant design-driving operational elements and characterizing them to the level of detail necessary to assess design impact. OPSITs are then developed to feature selected operational characteristics, or combinations thereof, in operationally viable combat environments. Inputs and reviews from the acquisition, operator, and intelligence communities ensure valid, realistic, and most importantly, useful representations.

Even following a similar development methodology, each DRM could present a different definition of the threat and operating environment that might, in turn, perpetuate or exacerbate interoperability problems caused in part by stovepiped designs. Thus coordination is required to link the DRMs so that the desired commonality and consistency are reached and the individual DRMs can focus the operational characteristics of concern on their respective programs. Figure 2 presents the relationship between Warfare Area and Platform DRMs.

Warfare Area DRMs (e.g., TAMD) focus on the application of single and multiwarfare platform types to a specific warfare area. Platform DRMs have an "orthogonal" orientation, as illustrated in Fig. 2 for the DD 21 DRM, i.e., they focus on the variety of warfare operating environments that might be encountered by a single multiwarfare platform. Battle Force DRMs focus on a multiwarfare, multiplatform system-of-systems

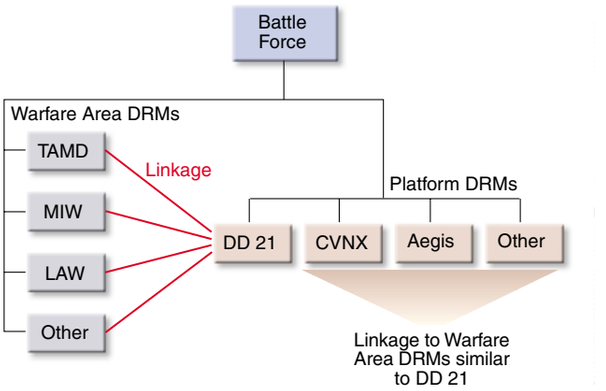

Figure 2. DRM relationships.

operating environment that provides a venue for cross-warfare area, cross-platform, and interoperability analyses. The overlap between a Warfare Area and Platform DRM is shown in more detail in Fig. 3. The Platform DRM covers only a subset of the Warfare Area DRM domain, where the threat and operational environments must be consistent. The Warfare Area DRM is developed to enable exploration of the entire warfare domain, which includes portions of the other Platform DRMs.

THE DRM CONSTRUCT

The previous section discussed the need for Warfare Area and Platform-centric DRMs and how they differ and complement one another. This section provides a more in-depth look at the content and structure of these products as well as a brief description of the Battle Force DRM.

Warfare Area DRMs

Figure 4 illustrates the basic construct for a TAMD DRM and is representative of a typical Warfare Area DRM. An overarching multiphase, Joint campaign provides a common framework to link OPSITs from, in this example, five mission areas or programs. In addition it provides a variety of available threat levels,

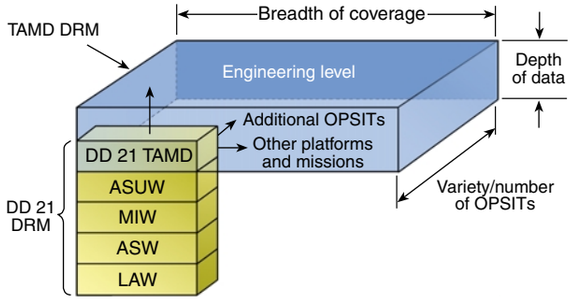

Figure 3. Warfare Area/Platform DRM commonality.

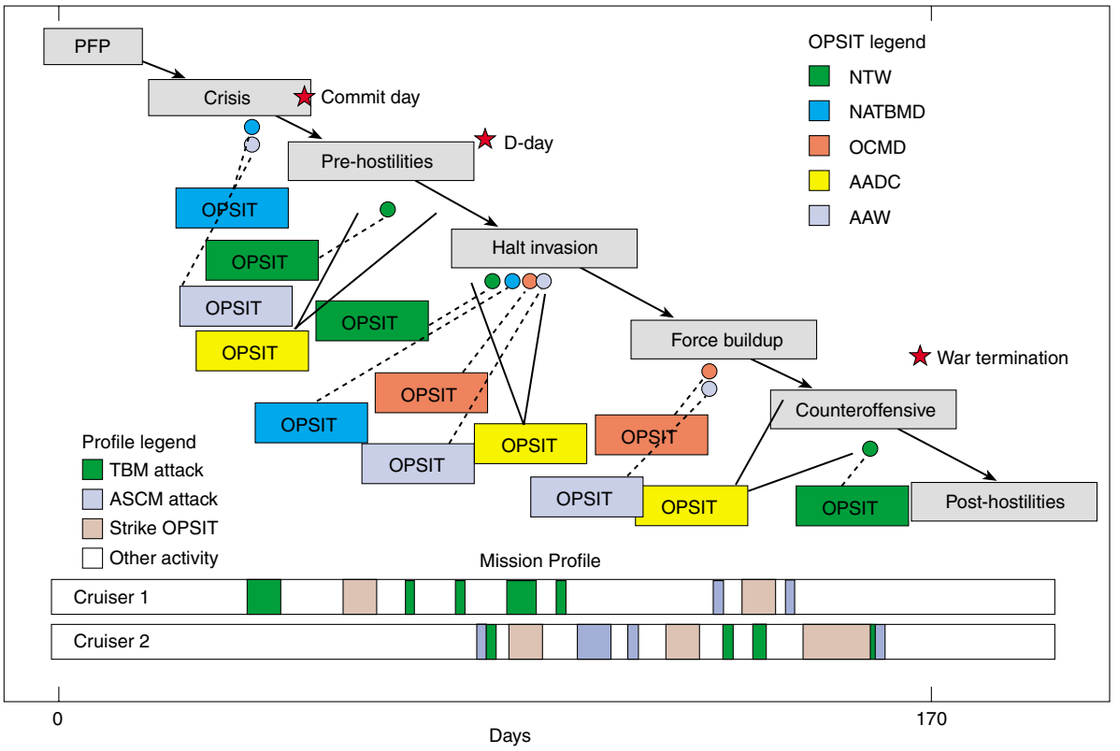

Figure 4. This TAMD DRM construct has four key elements: (1) Joint campaign context, (2) OPSITs, (3) threat/physical environment characterization, and (4) Mission Profiles. Five OPSITs are considered here. (NATBMD = Navy Area TBMD, PFP = peacetime forward presence.)

attack geometries and sizes, and weather conditions; Blue Force composition, missions, and locations; and BMC^{4}I (battle management, command, control, communications, computers, and intelligence) options. For warfare areas encompassing multiple major mission areas and programs (e.g., TAMD), an overarching document will outline the campaign and describe the DRM concept, uses, assumptions, methodology, and elements common to all missions within that area. The OPSITs, along with related threat, operational, and physical environmental data, will reside in program-specific annexes to the DRM. The TAMD DRM has four key elements, which are detailed in the following discussion.

Joint Campaign Context

To ensure that OPSITs are widely accepted as realistic and viable, they are set in a Joint campaign context based on Defense Planning Guidance (DPG) Illustrative Planning Scenarios (IPS). The selected Joint campaign presents multiple conflict phases and the largest available theater to supply the required breadth of physical environments, threat geometries, and geography. This is done to minimize the potential that region-specific characteristics could inadvertently restrict trade-offs and result in a "single-point design" of limited capability. The Joint campaign also presents a diversity of conditions that could be encountered by a system of systems in the context of deployment cycle, logistics, and asset availability. The use of several DPG IPS involving different theaters may be needed to yield the desired variety of threat and environmental conditions.

OPSITs

OPSITs are discrete multi-engagement events with specified operational characteristics (Table 1). They include the threat systems, engagement geometry, and related tactics. As an initial condition, each OPSIT also specifies the location and status of applicable Navy and Joint/coalition assets, assigned missions to include the defended area, connectivity to BMC^{4}I elements outside the system boundaries, the status of noncombatants, and a characterization of the physical environment.

Mission-specific families of OPSITs merge the appropriate threat, natural, and Blue Force information into a single, coherent, and comprehensive depiction of the potential OPSITs for the system in development. The use of discrete OPSITs provides a set of fixed "test points" that collectively yield a representative sampling of the problem space. Users are encouraged to conduct a parametric exploration of the problem space to aid concept definition, with the understanding that

Table 1. OPSIT content.

Operational characteristics	Information
Blue Force locations	Mission area assets Other Navy/Joint assets Potential cue sources
BMC^{4}I	Operational mode Architecture Connectivity
Joint campaign context	DPG-based scenarios Force flows Multiphase conflict
Physical environment	Weather Geography Space, air, sea background
Threat characterization	Performance Signatures Countermeasures
Threat tactics	Raid size Attack timing Attack coordination

proposed solutions will be evaluated against the common baseline defined by an OPSIT family.

OPSITs are specifically developed to stress selected system design attributes and support functional and performance trade-off analysis (e.g., radar range vs. interceptor kinematics). Each OPSIT will focus on one or more stressing operational characteristic, such as threat, which in turn supports a specific functional trade area. Operational characteristics generally fall into one of the following broad categories: technical threat characterization, threat tactics, physical environment, or Blue Force employment (which includes the campaign context, force locations, and BMC^{4}I).

OPSITs are identified based on Mission Needs Statements, Operational Requirements Documents, System Requirements Documents (of both the system and its host platform), DPG, intelligence, and Fleet feedback. The family of OPSITs is built to enable broad application in support of the systems engineering process including design trade-offs, modeling and simulation, and analysis of the engineering performance parameters.

A single OPSIT family, however, is inadequate to meet the stated DRM objective to support the program through its lifetime. And OPSITs developed early in the program have been found to be inappropriate to support the latter stages. A minimum of two OPSIT families are therefore needed: (1) a developmental family to support concept development, requirements definition, and related trade studies, and (2) a performance assessment family that serves as the official baseline for modeling and simulation, performance verification, test and evaluation, training, and exercises. The developmental family defines the broadest problem space consistent with physical limitations and projected worldwide threat systems. This enables early systems engineering efforts to determine "knees in the curve" and to define sufficiently robust requirements. Once requirements are established, a performance assessment family is developed to populate the smaller problem space. These performance assessment OPSITs are constrained by the system requirements and approved intelligence projections. Some developmental OPSITs are expected to be captured by the performance assessment family and provide an added link between the two families.

Threat/Physical Environment Characterization

Threat characterization includes specific threat performance characteristics and signatures, along with related countermeasures that define design-driving parameters. The DRM documents the range of threat parameter values as determined by an uncertainty analysis and associated confidence levels to facilitate an understanding of threat parameter variations. This helps the program manager identify solutions that exploit low-uncertainty and high-confidence (stable) threat characteristics and "red flag" alternatives that have high sensitivity, potential volatility, and/or low-confidence characteristics. Existing or projected threat systems are selected to populate the range of parameter values. Engineering excursions are identified where threat developments are likely and technically feasible but not projected by the intelligence community. The intelligence community is tasked to review the engineering excursions and to assess their technical and economical feasibility.

Threat characterization also involves comparing available intelligence community data to the data required at the engineering level to perform system design trade-offs and modeling and simulation. If shortfalls are identified, the DRM works within the threat engineering process prescribed by the cognizant warfare area PEO (and in close cooperation with the intelligence community) to perform threat engineering and analysis to fill the identified deficiencies. All derived threat parameters are provided by the government via the cognizant PEO, and the derived parameters are clearly identified in the DRM.

To characterize the physical environment, emphasis is placed on the provided authoritative data that are of appropriate fidelity and format for the proposed models and program applications. A major goal of this effort is to supply data consistent with the threat characterizations and the OPSITs as well as a singular

representation to ensure that the strongest possible baseline is maintained for systems engineering.

Mission Profile

The Mission Profile (notionally shown across the bottom of Fig. 4) is intended to serve as an activity log for selected system elements. Similar to the Functional Mission Profile in the DRMP, the Mission Profile documents the number, nature, and duration of significant combat and noncombat activities throughout the campaign. Combat activity will reflect the OPSITs as well as additional combat events not captured in the OPSITs. Noncombat operations include movements and reload/replenishment activities. The Mission Profile is intended to offer a common baseline to enhance the consistency of results across the program.

Platform DRMs

As previously discussed, Platform DRMs differ from Warfare Area DRMs in that the focus is shifted to a single platform type required to conduct and support a variety of operations spanning multiple warfare areas. In most cases, it is not plausible to expect a platform to perform its full range of required operations, which normally include combat and noncombat activity, in a single campaign. In addition, the platforms generally must operate across a broader spectrum of environmental conditions than those found in a single theater. These requirements lead to DRMs that are characterized by an ensemble of dissociated, warfare area/operation-specific OPSITs located around the globe. The DD 21 OPSITs range from South America to Asia, with operations from counterdrug to land attack during a major theater conflict.

The DD 21 DRM translates government system requirements into an operational context. The context is given to competing industry teams as the threat and operating baseline that will support concept evaluation and ultimately contract award. The DD 21 OPSITs are linked to the DPG IPS and contain specific engagements presented as both independent and concurrent operations.

Again, Platform DRMs do not offer the breadth of coverage, variety/number of OPSITs (there are only a few, if any, dedicated OPSITs in each warfare area), nor the depth of detail (OPSITs, threat, and physical environment are less well defined) provided by any given Warfare Area DRM. The Platform DRM does, however, provide a slice across warfare areas, and as such can serve as a conduit to explore means to increase coordination and interoperability among traditional warfare area stovepipes.

Battle Force DRMs

Although the environments of Warfare Area and Platform DRMs involve other Navy and Joint/Allied forces, they are still tightly focused on their respective concerns and do not yield an adequate basis for the exploration of one of the Navy's biggest issues—interoperability. As the Navy structures itself to fight alongside other services as a system of systems, and ultimately as a single, fully integrated Joint system, interoperability shortfalls become more than nuisances or complications; they become disablers. The Naval Sea Systems Command initiated the Battle Force Engineering Initiative to, in the short term, fix existing problems and, in the long term, "design in" interoperability to avoid future problems. The Battle Force DRM is a fundamental first step in that long-term process.

As with any DRM, the objective of the Battle Force DRM is to define the threat and operational environment, in this case, for a battle force. Since all the warfare area systems and platforms are part of the battle force, the challenge for the Battle Force DRM is to create multimission, multiplatform OPSITs that are consistent with the OPSITs developed in other DRMs. The approach is to elevate OPSITs or portions thereof to the battle force level and combine them in situations expected to stress coordination and highlight interoperability issues.

SUMMARY

The "new world order" brought on by the end of the Cold War has significantly changed the rules of the game. The players are different: a large, monolithic, generally predictable peer adversary has been replaced by a disparate array of nations and other groups with often competing agendas. The rules are different: fewer countries are able, or willing, to directly challenge the United States militarily, and thus will develop asymmetric means to exploit perceived weaknesses. Even the game board has changed: the Navy, in particular, must now be able to operate effectively in a demanding littoral environment. In this environment, ships are exposed to a significantly increased number and variety of threats, reaction times are shorter, unique physical environment challenges are posed, and a more complex tactical situation exists that may often be more complicated by Joint/Allied operations and/or political constraints. The challenge for the Navy is to develop sufficiently robust and flexible, yet cost-effective, solutions that can efficiently maintain maritime supremacy in the littoral environment.

To meet this challenge, the Navy needs effective means of problem solving, or systems engineering, which in turn hinges on accurate and appropriate problem definition. The best solution in the world may be worthless if it solves the wrong problem. An insufficiently defined problem may be as dangerous as an inaccurate one, as it will spawn a multitude of potential solutions. Problem definition driven by a preordained

solution will only serve to bias against potentially better alternatives.

The DRM concept seeks to define the problem, not the solution. A DRM defines the authoritative projected threat and operating environment baseline for a specific platform or warfare area. The DRM approach is to identify and characterize the significant elements of threat systems, tactics, the physical environment, and the Blue Force environment at various levels of fidelity to support a wide range of systems engineering tasks. In addition to detailed characterization of the appropriate threat systems and physical environment, a DRM presents a set of discrete OPSITs, each of which provides a comprehensive description of a single event or in some cases a limited period of activity, that collectively define the problem space. As a program matures and system requirements are established, a DRM will develop a new family of OPSITs to reflect the appropriate problem space and support the evolving needs of the systems engineering process.

Since the beginning of warfare, successful military leaders have recognized the importance of knowing the enemy, knowing the terrain, and knowing themselves. The complexity and variables associated with future military operations, particularly naval operations in the littoral environment, make this knowledge base even more critical to ensure that the U.S. Armed Forces are developing the right weapons systems to accomplish their assigned missions. From providing the baseline for trade studies leading to the development of the requirements for the NTW TBMD system to establishing a common operational context for competing DD 21 design teams, the DRM concept has shown it can make positive contributions to that knowledge base. As other program managers embrace the DRM concept and make similar successful applications to their programs, the family of DRMs continues to expand within the Navy and potentially to other service and Joint programs. Logically, the DRM concept could evolve into a tightly woven suite of consistent products that would define an operationally viable, common baseline to support the development of all U.S. weapon systems and platforms in a fully integrated, Joint system-of-systems context.

REFERENCES

[1] *Interim Standard on Systems Engineering*, EIA/IS-632, Electronic Industries Association, Engineering Dept., Washington, DC (Dec 1994).
[2] *Transition from Development to Production*, DoD 4245.7-M, Assistant Secretary of Defense for Acquisition and Logistics, Washington, DC (Sep 1985).
[3] *Best Practices, How to Avoid Surprises in the World's Most Complicated Technical Process*, NAVSO P-6071, Department of the Navy, Washington DC (Mar 1986).

THE AUTHORS

FRED R. SKOLNICK has a B.S. in electrical engineering from Drexel University and an M.S. in systems engineering from George Washington University. He rejoined APL in 1980 and is a member of the Principal Professional Staff and Supervisor of the Mission Analysis Group in the Joint Warfare Analysis Department. Mr. Skolnick has been instrumental in the development of a number of efforts that define the operational context for Navy combat systems including the *Surface Warfare Threat Handbook*, *Littoral Warfare Handbook*, Theater Air and Missile Defense DRM, and Battle Force DRM. His e-mail address is fred.skolnick@jhuapl.edu.

PHILLIP G. WILKINS is a Senior Staff member of APL's Joint Warfare Analysis Department. He holds a B.S. in engineering from Purdue University and an M.S. in aeronautical engineering from the Air Force Institute of Technology. Since joining APL in 1997, he has been involved in the development and evolution of the DRM concept and currently serves as the Project Manager and Technical Leader for the Theater Air and Missile Defense DRM. His e-mail address is phil.wilkins@jhuapl.edu.