Simulation Approaches for Supporting Tactical System Development

Bruce L. Ballard, Robert E. Elwell Jr., Robin C. Gettier, Francis P. Horan, Arthur F. Krummenoehl, and Dawn B. Schepleng

Simulators play essential roles in the development of modern Navy combat systems. Simulators provide an environment wherein articles being tested operate under the same stimuli as would be applied in a deployed configuration. The simulators' levels of fidelity range from basic interface functions to sophisticated interactions among multiple systems in a battle group. This article summarizes technology application for the Laboratory's simulator work associated with the Cooperative Engagement Capability and Ship Self-Defense System programs over the past several years; it also addresses simulator computer architecture, fidelity, hardware-in-the-loop, software-in-the-loop, DoD High Level Architecture, and accreditation.

INTRODUCTION

A simulator is a model that exhibits the behaviors of a particular system when provided with a collection of controlled inputs.[1] Simulators, therefore, can be useful substitutes for real systems when the real system is unavailable or ill-suited for the task at hand. They are typically used in place of real systems to reduce costs or improve capabilities. Cost savings are usually realized because specific aspects of a system's behavior can be replicated adequately for a certain task without having to provide a complete, real system. As long as a simulator's limitations are understood, it can be an effective substitute. Capabilities can be improved in many areas, but three key areas are testing, facilitating evaluation of "what-if" scenarios during system development, and serving as effective trainers to support deployments.[2]

The Wrap-Around Simulation Concept

A wrap-around simulator is a collection of simulations operating in a coordinated manner that support one or more systems under test. Wrap-around simulators at APL have been used extensively for problem solving in the anti-air warfare arena. In the anti-air warfare problem space, wrap-around simulators perform several principal and distinct functions (Fig. 1). The scenario scripting function captures the user's test scenario and transforms this scenario into a form suitable for processing by the models in the simulators. An entity generator "flies" simulated objects in accordance with the scenario script. For each object, this generator provides information such as kinematic data updates, radar cross section (RCS), and identification, friend or foe (IFF) codes to the simulators. Sensor models within the sensor simulations transform the simulated aircraft and missile data to
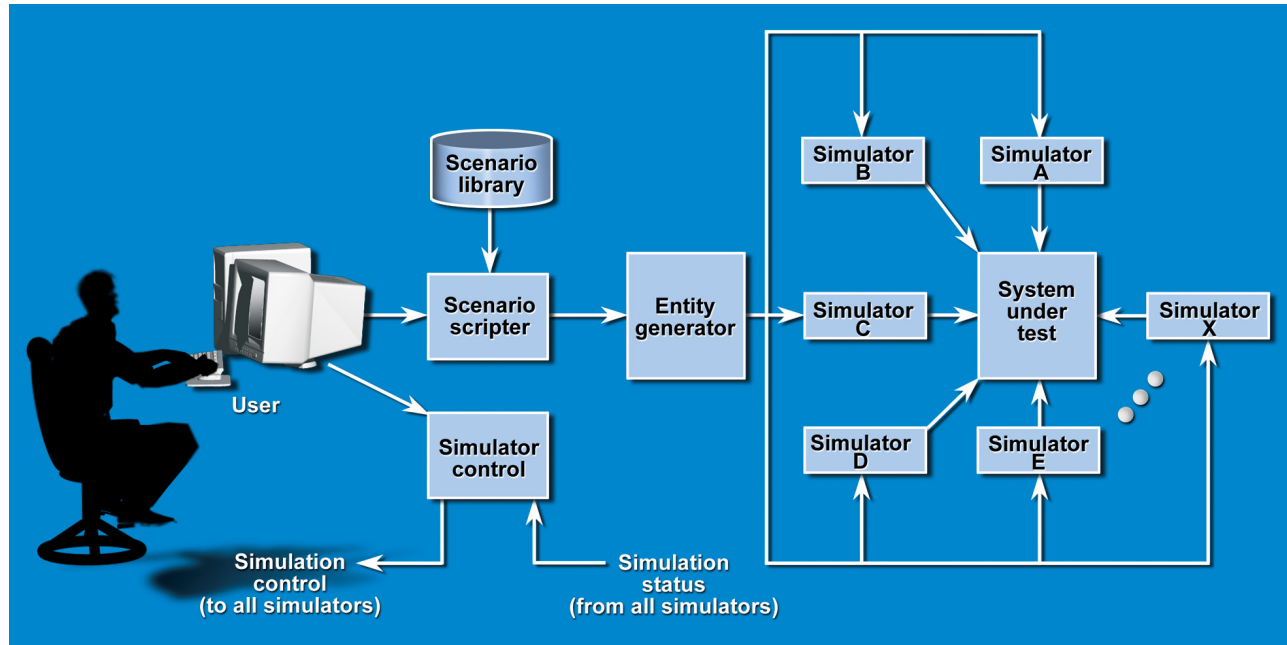
Figure 1. Typical wrap-around simulator functional block diagram.

simulated sensor returns, taking into account the effects of the operating environment specified in the scenario; sensor interface functions then convert the model outputs into the exact signals required by the system under test. Simulators can also represent weapon element, tactical communications link, and control system functions. The combination of these functions operating with the sensor functions serves to wrap around the system under test, satisfying all interface requirements needed to support particular tests. The scenario scripting function also defines simulated operating characteristics of the weapon element and control system functions. The entity generator, in addition to driving the sensor models, provides "targets" to weapon simulations and simulated object data needed by the communications link and control system functions.

An extension of this wrap-around concept is shown in Fig. 2. This approach is quite effective for testing multiple systems that must share information and respond to the common environment in a coordinated fashion.

Applying Concepts to Solve Problems

As Navy combat systems have become more sophisticated over recent decades, the task of testing these systems to validate proper performance and interoperability at a reasonable cost has become more challenging. APL has been helping to meet that challenge by developing innovative approaches to supporting critical experiments, weapon system development, and operational validations through the use of simulators.

Two hallmarks of APL's work on simulators are the judicious application of the latest technology and the foresight to ensure that solutions implemented today can be easily adapted to satisfy evolving requirements. The Cooperative Engagement Capability (CEC) and Ship Self-Defense System (SSDS) are two programs with which APL has been broadly involved for over a decade. To support these programs, APL applied modeling and simulation (M&S) technologies to solve numerous challenges at a wide variety of levels. This article summarizes simulation design considerations, the application of simulator technology to a selection of the problems faced by APL's sponsors, and how APL has helped to instill confidence in these simulations by working with the Navy to successfully accredit them. The topics are grouped according to technical areas as follows:

- The first area, Capability and Design Considerations, describes factors that can affect simulation capabilities and design.
- The second area, Accreditation, describes the work performed to obtain formal Navy certification of specific simulation capabilities.
- Next, Architectures focuses on challenges APL's sponsors faced where the computer and software architecture figured prominently in their solutions.
- The fourth area, Simulation Fidelity, focuses on challenges where simulation fidelity played a key role.
- The fifth area, Real-Time Sensor Modeling for Probability of Raid Annihilation Analysis, describes an approach for integrating high-fidelity simulations and legacy systems to determine the performance of a ship defending itself against a cruise missile attack.
- And finally, High Level Architecture Support addresses involvement with the Navy simulation
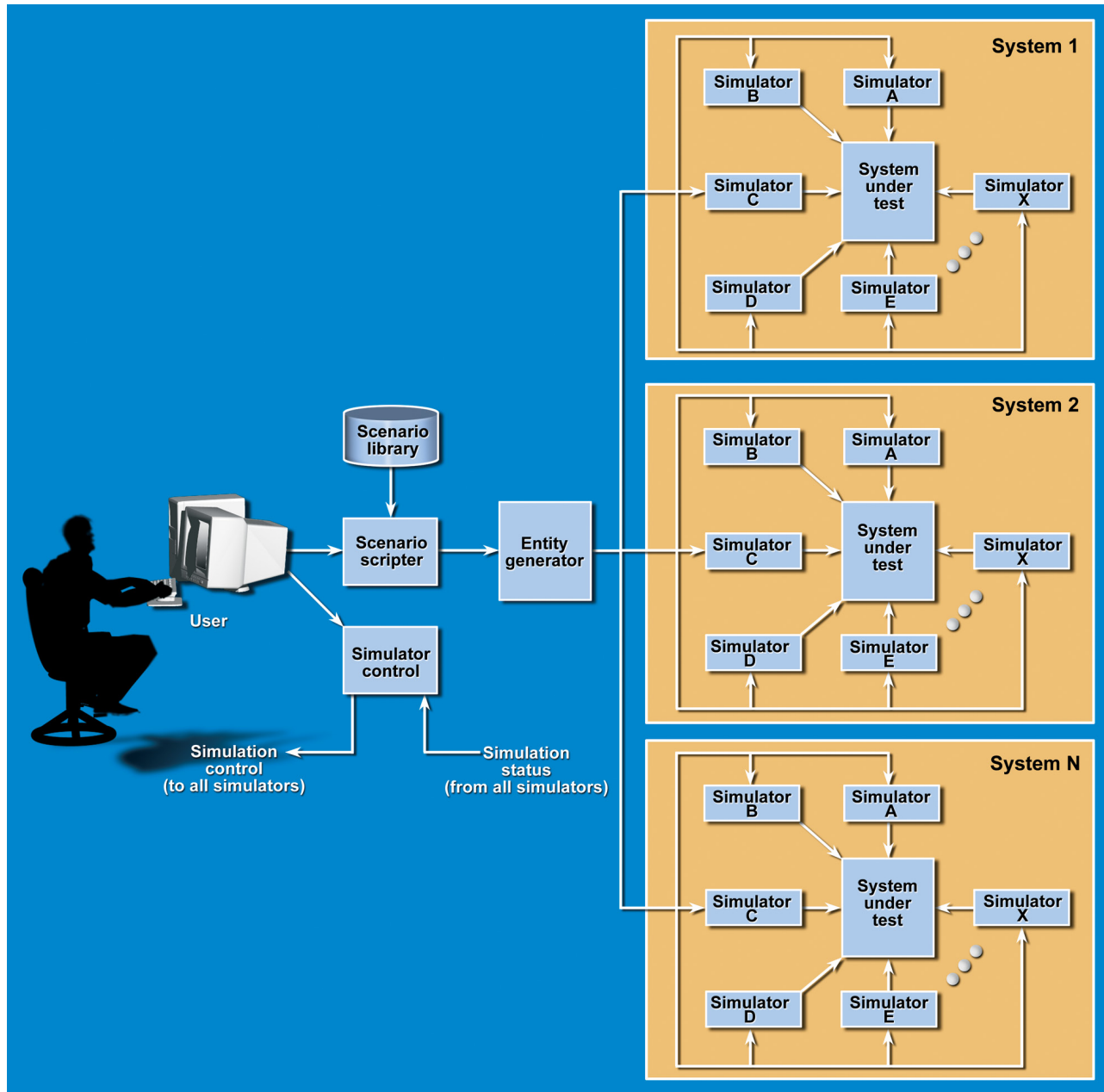
Figure 2. Typical wrap-around simulator functional block diagram (multiple system configuration).

community in implementing a simulation interoperability standard called the High Level Architecture (HLA).

Each topic in an area that describes a specific solution provided to a customer begins with a requirement statement to help put the topic into context.

CAPABILITY AND DESIGN CONSIDERATIONS

Requirements for simulators and their design approaches depend on many factors. A principal driver is the complexity of the systems under test. Complexity

of defensive systems is driven by increasingly sophisticated threat capabilities. For example, an enemy air or surface unit capable of launching an anti-ship cruise missile might employ self-screening jamming to deny range information to the attacked ship, thereby delaying self-defense actions. An automated defense system might use a triangulation method to obtain range to the threat by receiving passive angle data from two or more ships transmitted among the ships over a high-speed data distribution capability. To test such a system in a laboratory, a simulator is needed that "flies" the threat with realistic altitude changes and maneuvers, models the jamming, models the sensor providing the jamming measurements

to the passive angle trackers under test, and provides instantiations of these models for all units (under test) that are part of the triangulation process. In addition, the simulator must provide an effective scripting capability to set up this scenario.

The number of threats a system under test handles simultaneously and the degree to which the system provides situational awareness to the tactical users can drive required simulator capabilities. During naval littoral operations there can be many friendly or neutral aircraft and surface units in the operating environment, but potentially no more than a few threats. The detection, tracking, and identification of all these objects simultaneously require correlating radar and beacon returns with individual tracks and displaying a large amount of information to the system operators in a sensible manner. A simulator used to test such a system must replicate this complicated environment of surface, air, friend, and foe entities and convert this representation to the appropriate sensor stimuli.

The mission performed by the system under test affects simulator requirements. For example, certain tactical systems are used in a stand-alone mode for self-defense, while others interact with systems on other combatants via tactical data information links to fuse or otherwise take advantage of detection information known by other units. For the latter applications, systems must interact with upwards of 10 other combatants that host similar, but not the same, weapon elements. The capabilities of each unit involve detection, tracking, and identification of aircraft in the surveillance volumes of several, but not all, units. Each unit hosts a set of sensors, some in common with those of other units, some not. Each unit hosts a combat decision system that aids operators in making decisions based on sensor and tracking information and allows them to control weapons and/or tactical aircraft. To test a weapon system that normally resides in this multiple-unit configuration, a simulator must represent the large part of the configuration that is not under test. The simulator must represent these "external" elements to the extent that they affect the data presented to the elements under test. The design of such a simulator might include the same test aircraft scenario-generation capability described for the previous littoral warfare case and, in addition, would contain radar and combat system models to represent the parts of the configuration not under test. Figure 3 shows a typical environment that could be synthesized for a combat system under test.

The availability of necessary test assets is another factor that influences simulator requirements. For testing systems in a multiple combatant battle group configuration, the collection of required systems is not available at a single site but is located at various facilities across the United States. The simulators supporting the tests are also distributed geographically and must perform the same functions previously described for
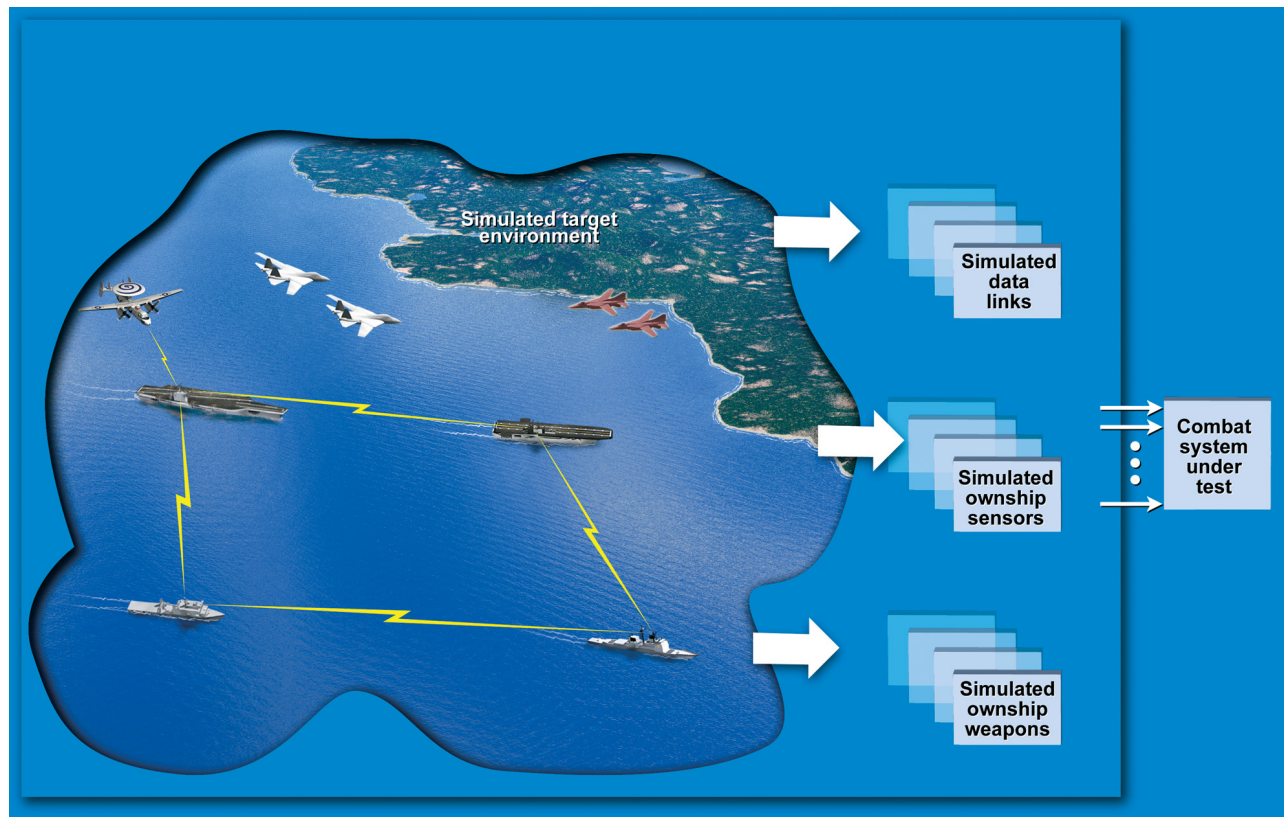

Figure 3. Typical simulated environment presented to a combat system under test using the Wrap-Around Simulation Program.

multiple unit testing. The design of such a simulator may use the same scenario scripter and entity generator applicable to testing a single system in the littoral scenario, but the simulation of each unit's elements under test must be done within the facility that hosts the combat system. To accomplish this, the single-scenario generator transmits "ground truth" information over a high-speed link to the simulator's radar models located at each (remote) site. The simulators at all sites must operate in time synchronism, which can be accomplished by synchronizing all simulators to the Global Positioning System or by a time synchronization protocol such as Network Time Protocol.

Phase of System Development

The development phase wherein a simulator is used can affect its design. For example, simulators may support preliminary analysis of performance improvements to sensor and weapon systems. System upgrades may involve modification or addition of sensors and/or combat system functions. Detailed requirements for the sensor and combat system processing are sought early before formal development of the modifications; often, prototype modifications of the sensor or combat system are made and a critical experiment is performed. Simulators support these efforts in two ways. First, once the critical experiment is performed and detailed sensor data are collected, the simulator can replay sensor data to analyze the refinement of the prototype modifications and algorithms. Second, a simulator that models threats (e.g., their kinematics and RCSs) and the upgraded sensor(s) can be used to apply a range of stimuli to the combat system under test, reflecting adjustments to the sensor processing and variations of threat characteristics.

A related application is that of analyzing legacy tracking systems when new information about threats emerges. A rapid method for ascertaining the performance of deployed systems is to model the newly revealed threat characteristics in the simulator and exercise the legacy weapon element(s) using the controlled environment of the simulator. Such tests, employing the simulator and the actual weapon system computers (a more complex environment than simply exercising the algorithms), provide a refined estimate of performance and are especially useful because the actual (deployed) weapon elements are exercised. The software design of the simulator must be very flexible to correctly handle the variety of data inputs and processing modeled.

ACCREDITATION

Requirement: Provide confidence in simulation results used to make key technical and programmatic decisions

Systems being acquired by the DoD are becoming increasingly expensive. As a result, the DoD is constantly looking for opportunities to reduce costs without jeopardizing program objectives. One method for reducing costs is to use M&S whenever appropriate. M&S techniques can be applied throughout the acquisition cycle from concept definition through manufacturing, testing, and training. DoD Directive 5000.1 states that M&S shall be used to reduce the resources, time, and risks of the acquisition process and to increase the quality of the systems being acquired.[3]

To reduce risks associated with using M&S in lieu of live assets for decision making, DoD Directive 5000.59 requires acquisition managers to establish verification, validation, and accreditation (VV&A) policies and procedures to manage the use of M&S in acquisitions.[4] Verification of the model or simulation ensures that it accurately represents the developer's specification. Validation of the model or simulation ensures that it behaves in a realistic manner for the purpose for which it is intended. (*Intended use* controls the extent to which the model or simulation must replicate the behavior of the real system, and it provides an effective way to bound the scope of a VV&A effort.) Accreditation is the process in which the DoD sponsor reviews the verification and validation results and certifies, or certifies with exceptions, that the model or simulation is ready for its intended use.

In 1999, the U.S. Navy CEC Program Office tasked APL to participate in accrediting the APL-developed Cooperative Engagement Processor Wrap-Around Simulation Program (CEP WASP). This effort recognized the role the CEP WASP would play as an M&S element supporting critical CEC technical and programmatic decisions. The scope of this initial accreditation effort was to certify that the CEP WASP would adequately support upcoming developmental tests and independent verification and validation tests. Because independent verification and validation relies on WASP for many test needs, the scope of this initial accreditation addressed many WASP functions associated with CEC testing.

APL worked closely with Navy accreditation team members to produce a verification and validation plan to document how the CEP WASP would be tested. The verification and validation tests were run and a formal test report was submitted to the Navy for review. As a result, the CEC Program Office issued a memorandum in February 2000 certifying that the CEP WASP was capable of supporting the upcoming tests.[5]

In the fall of 2000, the CEC Program Office again tasked APL with a WASP accreditation effort, this time to support the CEC technical and operational evaluations. During these evaluations, live assets are used for testing as much as possible and reliance on M&S is minimized. For these tests, the CEP WASP's role was limited to those tests for which it was impractical to use live assets. These tests typically involved evaluation

of system performance under high track loads or while tracking and engaging air targets.

APL followed the same path as the 1999 accreditation effort; however, because the scope of the test for the CEP WASP was more limited, the scope of the VV&A effort was also limited. The verification and validation tests were run, and a new report was submitted for review in November 2000. The WASP was accredited in November 2000, and an amended accreditation to reflect a different test configuration was received in April 2001.[6,7]

ARCHITECTURES

The simulation architectures developed by APL to support tactical systems are driven by customer needs. As the complexity and connectivity of battle forces and their associated combat systems have increased, simulation architectures have been evolving to meet these new challenges. (For more details on constructing a typical WASP simulation, see the boxed insert.)

Multiple-Site Wrap-Around Simulation Programs

Requirement: Provide a capability to support distributed land-based battle group interoperability tests, thereby reducing the costs associated with live at-sea tests

By its very nature, the CEP has a tremendous variety of test requirements. To perform adequate test, certification, and demonstration of the system, live assets are imperative. However, these assets are extremely expensive. Also, the time available aboard Navy combatants and at certain land sites is very limited.

There are four types of developmental tests for the CEP: interface or algorithm testing, stand-alone testing with combat systems, stand-alone testing with live sensors, and battle group interoperability testing. The first three types of tests are performed using self-contained, land-based test sites. The fourth type of test is more difficult to execute. Its objective is to test and verify the CEP, combat system(s), tactical data links, and Data Distribution System (DDS) and to demonstrate that they can interoperate in a networked configuration. (The DDS provides the high-speed wireless network between CEC units for information exchange.) The assets required for this type of test increase significantly over the other test types, and multiple facilities must be connected to test a variety of battle group configurations.

To facilitate such a test, a common track picture was needed with either live or simulated sensor inputs to verify the CEP tracking functions. This testbed would be invaluable, providing back-to-back combat system testing with Aegis and non-Aegis combat systems in a typical CEP battle group configuration. CEP and combat system concepts like automatic track identification, track

number management, and engage-on-remote could be readily tested and demonstrated.

Given its architecture and that it was already installed at required test sites, the CEP WASP was a clear candidate for providing such a distributed simulation capability that could link many different CEP-equipped sites around the country. If a wide-area network were available among the sites, a single so-called "master" site could provide a single point of scenario control. The CEP WASP team demonstrated this very concept using an existing T1 line between the Navy's Aegis Computer Center in Dahlgren, Virginia, and Surface Combat System Center on Wallops Island, Virginia. The demonstration was the first of its kind for the CEP WASP and essentially proved that the CEP WASP could be configured to drive multiple, geographically displaced CEPs using a common simulated target picture. The distributed WASP was deployed quickly with minimal software changes and no hardware modifications.

The distributed WASP successfully supported tests of composite tracking, engagements, simulated network controls and communications, and track loading of the CEPs at two physically displaced locations. Although this test used only WASP assets, the notion of linking multiple distributed test sites with WASP, sharing ground truth data using an industry standard network interface, and plugging in other non-WASP simulated components seemed a natural extension.

Almost concurrently with this demonstration, an effort was undertaken by the Naval Sea Systems Command to put a more capable wide-area network into place, primarily to allow for battle group interoperability testing of various Navy combatants using a simulated tactical data link network. This network infrastructure was referred to as the Distributed Engineering Plant (DEP). The network medium was a combination of landlines and a higher-bandwidth backbone that was truly scalable. The DEP team conceived the notion of using the DEP network to broadcast ground truth entities to numerous simulation programs using the IEEE Standard 1278.1 Distributed Interactive Simulation (DIS) interface,[8] and to support the tactical data links among the combat systems to form a distributed testbed. The testbed would be used to test battle group interoperability using an Aegis combat system and an Advanced Combat Direction System interconnected via tactical data links. The target picture would be simulated and the data link communications would be implemented using the land network.

Shortly after this testbed was demonstrated, it became desirable to integrate the CEP. Given that the CEP WASP had already demonstrated execution in a distributed environment, a plan was formulated to incorporate the CEP WASP into the DEP. By April 1999, the concept was successfully demonstrated at four CEP-capable land-based test sites: the Aegis Computer

Center in Dahlgren, Virginia; the Surface Combat System Center on Wallops Island, Virginia; the Combat Direction Systems Activity in Dam Neck, Virginia; and the Integrated Combat System Test Facility in San Diego, California. The DEP infrastructure could now be used to combine the assets of the original DEP testbed with all of the CEP assets at those facilities. Finally, the difficult requirement of testing battle group interoperability with the integrated CEPs, combat systems, and tactical data links could be realized in a distributed testbed without consuming precious shipboard resources. The testbed has been used extensively for system development, independent verification and validation testing, developmental testing, and operational testing of the CEP with the combat systems.[9]

During the DEP system integration, APL continued to enhance and refine the WASP capabilities to provide better user interfaces, especially at the remote sites where there was no user control. The WASP team developed a software package where each simulation function implemented its own Web pages viewable on a Web browser running on the CEP WASP workstation at the site. These pages allowed the testers at any one site to closely monitor or troubleshoot the CEP WASP assets at other sites.

The CEP WASP continues to play an active role in DEP testing. In April 2000, a fifth CEP site, the Patuxent River Naval Air Station, Patuxent River, Maryland, was added to the DEP network.

Weapon Element Simulations and Integration with Industry

Requirement: Develop affordable test capabilities for the Ship Self-Defense System

By the mid-1990s, the maturity and capabilities of the CEP WASP made it a natural choice for supporting APL's development of the SSDS Mk 1. The SSDS integrated shipboard sensor, combat decision, and weapons elements into an automated sensor-to-shooter capability supporting defense against anti-ship cruise missiles. The SSDS Mk 1 WASP evolved from the CEP WASP and expanded the suite of simulations to include SSDS-specific own-ship and weapon simulations in addition to the sensor and command and control simulations of the CEP WASP. This WASP configuration was the first implemented through a joint effort by APL and industry. The SSDS prime contractor, Raytheon Naval and Maritime Systems Division, San Diego, California (then Hughes Aircraft Corporation), designed and provided select simulations, which were integrated in accordance with the WASP architectural design established by APL. In this way the subject matter expertise of both organizations was effectively used.

As part of the SSDS Mk 2 development program, APL, as the Navy's Technical Direction Agent, applied its experience with the SSDS Mk 1 and the WASP to the issue of how to support development and test of the SSDS Mk 2 in a cost-effective way. APL teamed with Raytheon (the SSDS prime contractor) and the Combat Direction Systems Activity, Dam Neck, Virginia (the testbed lead and co-developer), to architect a testbed that maximized software reuse from the SSDS Mk 1 WASP and CEP WASP, while minimizing the coupling between the new and old simulations to reduce the development risk. The resulting architecture combines the SSDS-unique simulations with those needed for the CEP, which interfaces with SSDS Mk 2. This architecture comprises simulations that wrap around SSDS Mk 2 and CEP together (i.e., as a single unit) or each individually. New simulations being developed by Raytheon and the Combat Direction Systems Activity for SSDS Mk 2 interface with the WASP via an IEEE Standard 1278.1 DIS interface.

Onboard Trainer

Requirement: Support the shipboard self-defense training mission using existing testbed simulators

To provide a cost-effective shipboard training tool for the SSDS Mk 1, APL worked with the Naval Performance Monitoring, Training and Assessment Program Office (PMS-430) to devise an architecture that maximized the reuse of simulation software that had been developed for testing purposes. The approach capitalized on the characteristics of the existing WASP sensor and weapon simulations; each simulation executed on a single-board computer compatible with the architecture of the tactical system, each simulation received target updates from a master source, and each simulation was capable of interfacing with the SSDS. Further, the performance requirements for simulation functions for the training application and the existing testbed were identical, allowing the simulation functions developed for the testbed to be used directly for the training application. An interface was provided from the existing tactical trainer to the entity generator of the WASP. The entity generator then accepted ground truth target updates from the trainer and distributed those updates to each WASP sensor and weapon simulation.

Although the SSDS Mk 1 training architecture met all its requirements, by design it did not allow training to be conducted during tactical operations. Under the SSDS Mk 2 and CEP programs, APL formulated an approach to allow training while the tactical systems are operating and the ship is under way. This approach explicitly tags training targets as training tracks and then injects these digitally into the CEP. Beyond the injection point, the message structures internal to CEP and SSDS supported the definition of a training track, so this message structure provided a path for incorporating the "artificial" training tracks. Because each training

track is thus positively identified, the CEP and SSDS are able to distinguish training tracks from live tracks and thus provide system handling appropriate for the track. In the fall of 2000, APL performed a critical experiment to demonstrate the fundamentals of this capability using the CEP.

Requirement: Build a WASP simulation: Joint service applications TPS-59 and Patriot

The TPS-59 radar and the Patriot air defense system are land-based anti-air warfare systems operated by the U.S. Marine Corps and U.S. Army, respectively. These systems extend the situational awareness and weapons coverage over land. APL developed WASP software and hardware to simulate these systems to support their integration with the CEP.

SIMULATION FIDELITY

The objectives of a critical experiment or operational evaluation in which a simulation is used determine the level of simulation fidelity required. During initial development of a tactical system, efforts focus on verifying interfaces to external systems and the internal communications infrastructure. Simplistic target profiles and benign environmental conditions are adequate for generating the interface message types and content needed.

As the system under test matures, a higher level of simulator fidelity is required to adequately exercise the algorithms implemented in the system. More complex target profiles are needed to replicate pertinent threat characteristics. The effects of various environmental conditions on system performance must be analyzed. The ability to correlate information from multiple sources has to be assessed. The challenge is to provide an adequate level of fidelity to meet requirements without introducing too much complexity. Because complexity tends to hamper usability, delay development schedules, increase the number of errors, and/or increase costs (sometimes prohibitively), unnecessary complexity is to be avoided.

Improved Threat Rendering

Requirement: Evaluate expected SSDS Mk 1 performance against representative threat targets prior to live-fire testing aboard the Self-Defense Test Ship

To conserve test assets and minimize the cost of live-fire testing of SSDS Mk 1 aboard the Self-Defense Test Ship, extensive analysis was performed to assess expected system performance before each test run. Unless the analysis results indicated that SSDS Mk 1 would perform satisfactorily, the test would not be allowed to proceed. (The remote-controllable Self-Defense Test Ship [EDDG 31] is a DDG 31–class ship that is used for testing the real SSDS against real anti-ship missiles.

The remote control capability allows the ship to operate unmanned during dangerous tests.)

To perform the analysis, the SSDS Mk 1 WASP had to replicate the threat profiles flown by the actual test target. The basic WASP target profile accommodates a limited number of time-tagged, first-order (i.e., constant acceleration) target maneuvers. However, the targets of interest included high-diving targets that continually change altitude and weaving targets that continually change heading. The task of manually scripting a complex threat profile as a series of simple maneuvers is tedious and generally produces inexact results.

To better render the threat profiles using the WASP, the capability to convert threat profile descriptions into WASP target maneuvers was added to the WASP scripter (Fig. 4). With this new capability, the WASP could accept a threat profile in the form of a table specifying the threat's position, velocity, and acceleration as a function of time. The WASP automatically determined the set of target maneuvers needed to replicate the profile. The conversion algorithm had to balance the fidelity with which the maneuvers matched the profile and the number of maneuvers used to not exceed the maximum number of target maneuvers handled by the WASP. This particular approach to improving threat rendering provided a level of fidelity that met the requirements for pre-test analyses. By leveraging the existing WASP capability to script simple target maneuvers, this approach could be implemented in a short period and at minimal cost.

Requirement: Evaluate performance of SSDS Mk 2 custom filter software

While SSDS Mk 1 required a higher-fidelity target-rendering capability for its operational evaluation, SSDS Mk 2 had a similar target rendering requirement to support its development. A significant portion of the Mk 2 development effort is being accomplished using the basic WASP scripting capability. However, integrating the more sophisticated algorithms used in SSDS Mk 2 required scripting more complex target profiles, and a slightly different approach was used to provide the required capability.
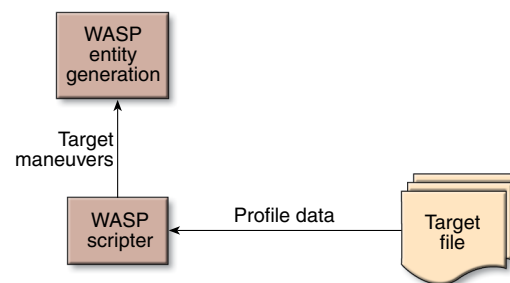

Figure 4. Converting threat profiles to WASP maneuvers.

SSDS Mk 2 uses custom data filters designed to extrapolate a target's kinematic state. These filters were developed using the MATLAB☐ commercial software package. A set of threat profiles was generated for input into the MATLAB development environment to test the custom filter algorithms. Once these algorithms had been ported to C++ and integrated into the tactical system, the filter software had to be tested against the same threat profiles to verify that the tactical filter software performed the same as the filter algorithm originally implemented in MATLAB.

Unlike the Mk 1 approach, which took advantage of the WASP's target maneuver feature, the approach chosen for Mk 2 leveraged the capabilities of the existing DIS interface in the WASP (Fig. 5). The DIS interface already had the capability to read a file containing DIS entity state data units and to feed those data into the WASP entity generator. The MATLAB threat profiles used for custom filter development were converted into the DIS entity state data file format. The integrated custom filter software was then tested against the same target profiles as the MATLAB version via profile data files processed by the DIS interface. In addition to minimizing the cost and schedule impact by leveraging existing WASP functionality, this approach was not limited by the maximum number of target maneuvers as was the approach used for SSDS Mk 1.

Improvements to Sensor Modeling

Requirement: Evaluate the "upspot" concept for the AN/SPS-49A surveillance radar as a means to provide threat elevation estimates

To deploy the Rolling Airframe Missile (RAM) Block 1 upgrade on SSDS Mk 1 ships, certain capabilities had to be added to SSDS Mk 1. One of the required enhancements was the capability to provide an estimated threat elevation to the missile launcher to counter higher-elevation threats.

Since the primary surveillance radar on the SSDS Mk 1 ships is the two-dimensional AN/SPS-49A, APL devised a concept that used the "upspot" capability of the radar to estimate the elevation of a threat. (The AN/SPS-49A radar reports range and bearing for contacts, but it is not designed to report elevation.) During normal operation, the radar rotates with its antenna pointed at a fixed elevation angle. When in upspot mode, SSDS commands the radar to periodically change the elevation pointing angle of the antenna. By taking into account the antenna pattern in the elevation plane, SSDS could analyze the changes in a target's apparent RCS as a function of antenna pointing angle to estimate the target's elevation. For example, consider a target positioned in the peak of the antenna's elevation beam when the antenna is at its nominal elevation pointing angle. During a scan when the antenna is pointed higher than its nominal angle, the target will no longer be in the beam peak. As a result, the power level of the target's radar return will be greater when the antenna is at its nominal pointing angle than when it is pointed higher. The magnitude of the change in the target radar return as the antenna elevation angle changes provides an estimator for the target's elevation relative to the radar.

The upspot technique would work best in a static environment, i.e., when the target is not moving, the target size is constant, radar noise levels are constant, and the ship is not pitching and rolling. Of course, SSDS does not operate in a static environment. Therefore, a significant analysis effort using the WASP was required to gauge the effectiveness of the upspot concept under normal operating conditions.

For most WASP applications, a simulation of the radar based on a probability of detection (PD)–driven sensor model is adequate. This model determines whether the radar detects a particular target on a given scan based on a fixed PD scripted for that target in the test scenario. In this case, simulated target detectability is neither a function of RCS nor of range from threat to the ship. The environmental effects are not modeled, nor is the elevation pointing angle of the antenna taken into account. This type of simulation is particularly useful for debugging tactical system software where analysis of the effects of radar fades or different sensor combinations on the overall composite track picture are not needed.

The PD-driven sensor model was not adequate for the upspot concept analysis. In this case, a higher-fidelity sensor model was needed. Rather than specify the target's (fixed) PD, the WASP was modified to allow the operator to script the target's RCS and type of Swerling fluctuation to be applied. The radar model then determined the result of each target detection opportunity based on a form of the radar range equation. The equation took into account the range from the radar to the target, the target's actual cross section (after applying the Swerling fluctuation), and the target's location within the antenna elevation beam pattern. Using the enhanced radar model, the analysis showed that the upspot concept provided an adequate target elevation estimate to allow
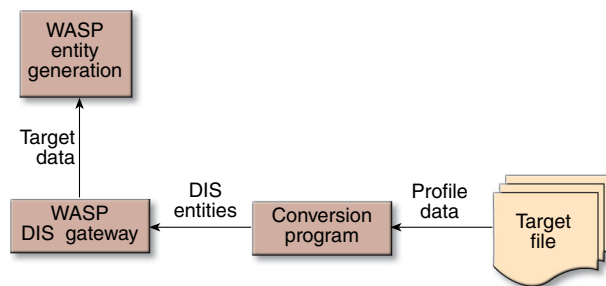

Figure 5. Generating threat maneuvers to WASP via the DIS interface.

optimal use of the missile's capabilities. Subsequent testing aboard the Self-Defense Test Ship was consistent with the findings of the analysis.

REAL-TIME SENSOR MODELING FOR PROBABILITY OF RAID ANNIHILATION ANALYSIS

Requirement: Devise a high-fidelity capability that could be used to assess self-defense effectiveness for the LPD 17 ship class

The SSDS Mk 2 WASP can be used as a component in a testbed to assess the probability of raid annihilation (PRA) for the LPD 17 and other ship classes. The PRA for LPD 17 is defined as the "ability of the standalone ship as a system to detect, control, engage, and defeat a specified raid of anti-ship cruise missiles with a specified level of probability in an operational environment."[10] PRA assessment encompasses threat, sensor, control system, and self-defense weapons represented by a combination of physics-based models, simulations, tactical hardware-in-the-loop (HWIL), and software-in-the-loop (SWIL). Figure 6 shows these interactions.

For the detect portion of PRA analysis, non–real-time high-fidelity threat and radar models have been used in the past to determine the sensor responses given a target's trajectory, kinematics, RCS, and environmental parameters. The resulting fixed set of sensor

detections was then applied to the tactical system (in this case, SSDS Mk 1) in real time by means of a "canned playback" capability of the WASP. For LPD 17 PRA analysis, it was initially proposed that this same method be used to create a sensor contact history file for threats of interest. This file would subsequently be input to the WASP, which would send the contacts in real time to SSDS along with other scripted WASP targets for background air traffic. One disadvantage of this approach is that with planned Monte Carlo scenario executions numbering in the thousands, the generation of thousands of contact history files would be extremely cumbersome and expensive. Another disadvantage of the approach is preclusion of growth to a capability for handling reactive targets, i.e., targets that change trajectories in the presence of countermeasures. A better solution is real-time integration of the high-fidelity detection models with the WASP.

This integration creates a high-fidelity, real-time sensor modeling tool to study PRA. This tool combines those aspects of the high-fidelity models and WASP that are most useful for PRA analysis and simulates the actual tracking and control elements of the LPD 17 in real time. Only one position history log per threat is needed; the Monte Carlo process is done within the WASP, where thousands of executions can be easily automated using a different random number seed for each execution. A capability for two near-simultaneous,
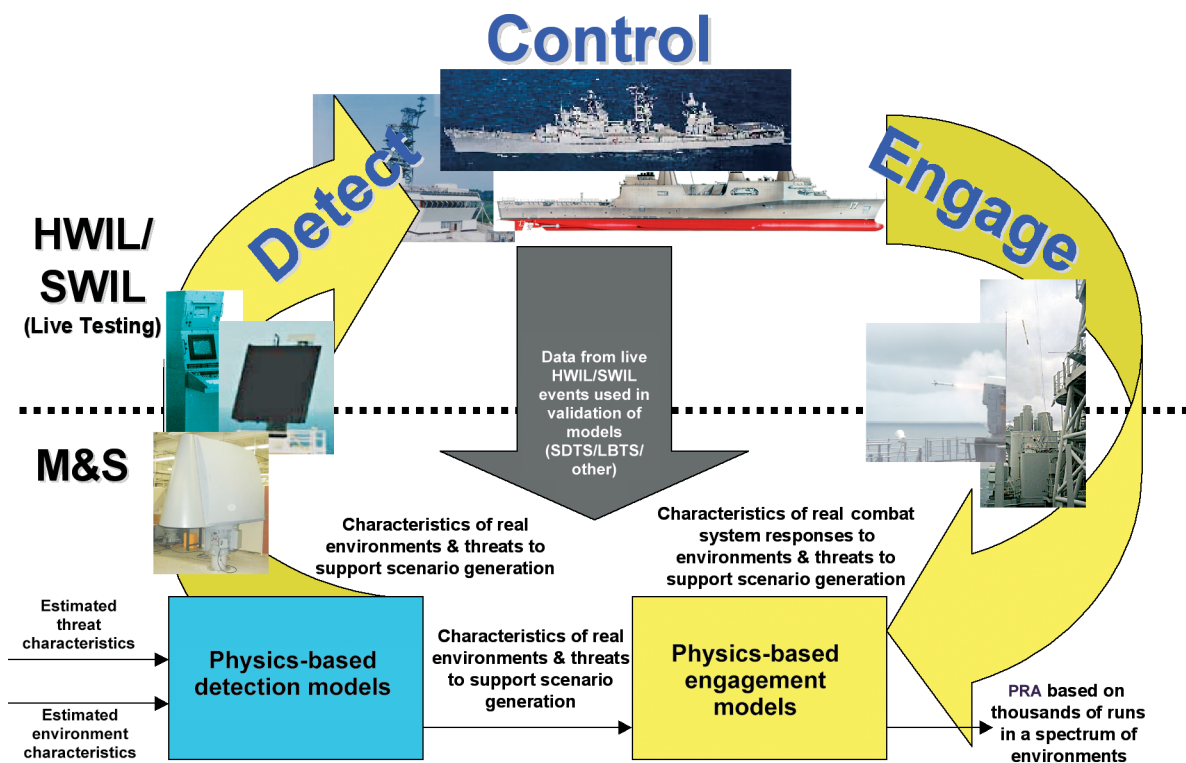

Figure 6. Interaction of models and simulations with HWIL/SWIL for PRA.

high-fidelity targets was built into the modified WASP. These high-fidelity targets can be either scripted using standard WASP scripting methods or fed into the Naval Research Laboratory's CRUISE model via a CRUISE-compatible scripting tool. (The CRUISE model accurately reproduces the trajectories of modern anti-ship cruise missile threats.) Regardless of how they are input, the targets are passed in real time to the high-fidelity models, which will compute detections in real time and also respond to sensitivity controls issued in real time by SSDS Mk 2.

This approach provides all the advantages of the standard WASP, including very flexible medium-fidelity (three-degree-of-freedom) entity generation for background air traffic, false alarms loading, ship motion, and sensor control. This combined real-time approach has become feasible with recent improvements in processor speed and memory capacity. The concept was first demonstrated in a critical experiment with the WASP and a high-fidelity model of the AN/SPS-49(V)5 two-dimensional surveillance radar.[10] With this approach, the WASP passes necessary target parameters to the high-fidelity radar models, which in turn simulate the detailed detection process in real time and, depending on the outcome, prompt the WASP to send or not send a radar detection report to the SSDS Mk 2.

In the high-fidelity AN/SPS-48E three-dimensional surveillance radar model, each radar beam in the vicinity of a target is modeled for frequency, transmitted power, elevation angle, and azimuth. The signal-to-noise ratio is calculated using propagation effects, antenna pattern, sensitivity time control, sea clutter, jamming, and an offset threshold calculated by the environment control function. The PD for each beam is calculated using a PD versus signal-to-noise curve. Finally, a Monte Carlo technique, which includes the effect of RCS fluctuations, determines the PD for the target in the vicinity of the modeled beams. Propagation effects are represented by a propagation factor based on antenna height, target altitude and range, sea state, frequency, polarization, vertical antenna pattern, and an effective Earth radius. The propagation factor is computed using digital terrain elevation data and the tropospheric electromagnetic parabolic equation routine to include the effects of ducting. Results from the latter are precomputed offline in non–real time for the planned target trajectory. Similarly, digital terrain elevation data terrain slices are selected offline for the planned target trajectory.

Additional fidelity improvements are planned for the AN/SPS-48E radar model, including land and sea clutter processing, bearing-dependent propagation, and improvements in signal processing modeling. Similarly, the fidelity of the AN/SPQ-9B horizon search radar model will be improved with full implementation of the lightweight antenna model and modeling of the back scan feature.

HIGH LEVEL ARCHITECTURE SUPPORT

Pilot Program for Probability of Raid Annihilation Analysis

Requirement: Demonstrate high-fidelity simulation technology to support analysis of integrated hardkill and softkill weapons for ship self-defense

In 1997, APL began work on the Integrated Ship Defense Advanced Distributed Simulation pilot program for the Program Executive Office Theater Surface Combatants. The pilot program used the High Level Architecture (HLA), a general-purpose methodology developed by the Defense Modeling and Simulation Office for reuse and interoperability of otherwise disparate simulations.[11] HLA services connect the simulations, termed *federates* in HLA parlance, into a grouping called a *federation*. In addition to the federation design, APL's major contribution to the pilot program was the SSDS Mk 1 federate. Other federates included threat, scenario control, AN/SPS-49(V)5 surveillance radar, RAM, and the Close-In Weapons System developed by other laboratories contributing to the pilot program.

Figure 7 shows the federation. The SSDS Mk 1 federate design involved transforming the real-time computer programs that execute in more than 10 microprocessors resident in several multiple processor VME chassis to operate in a single workstation. This design captured the actual tactical computer programs and allowed them to operate in a low-cost HLA-compliant workstation environment. The resultant SSDS Mk 1 federate interfaced via the Runtime Infrastructure (RTI) with the other federates; the federation operated at less than real time to give the compute-intensive, high-fidelity simulations the necessary time to complete their processing. The RTI is the software that implements the HLA services for coordination and data exchange, using a publish/subscribe paradigm. The original tactical code of SSDS Mk 1, which relied on a physical clock, was modified to synchronize with the other federates and infrastructure time using a time advance server. This server operated on a time request/time grant scheme. The real-time operating system had to be emulated in the non–real-time workstation environment. The very limited source code modifications were accomplished in the least intrusive manner and were automated predominantly using Perl scripts. This approach was taken so that the tactical code under configuration management would not be impacted and future SSDS program versions could easily be ported to the workstation environment using the same automated technique.

PRA analysis for Navy ships equipped with SSDS Mk 2 could also be achieved using an HLA federation. The method is as follows. The high-fidelity models of
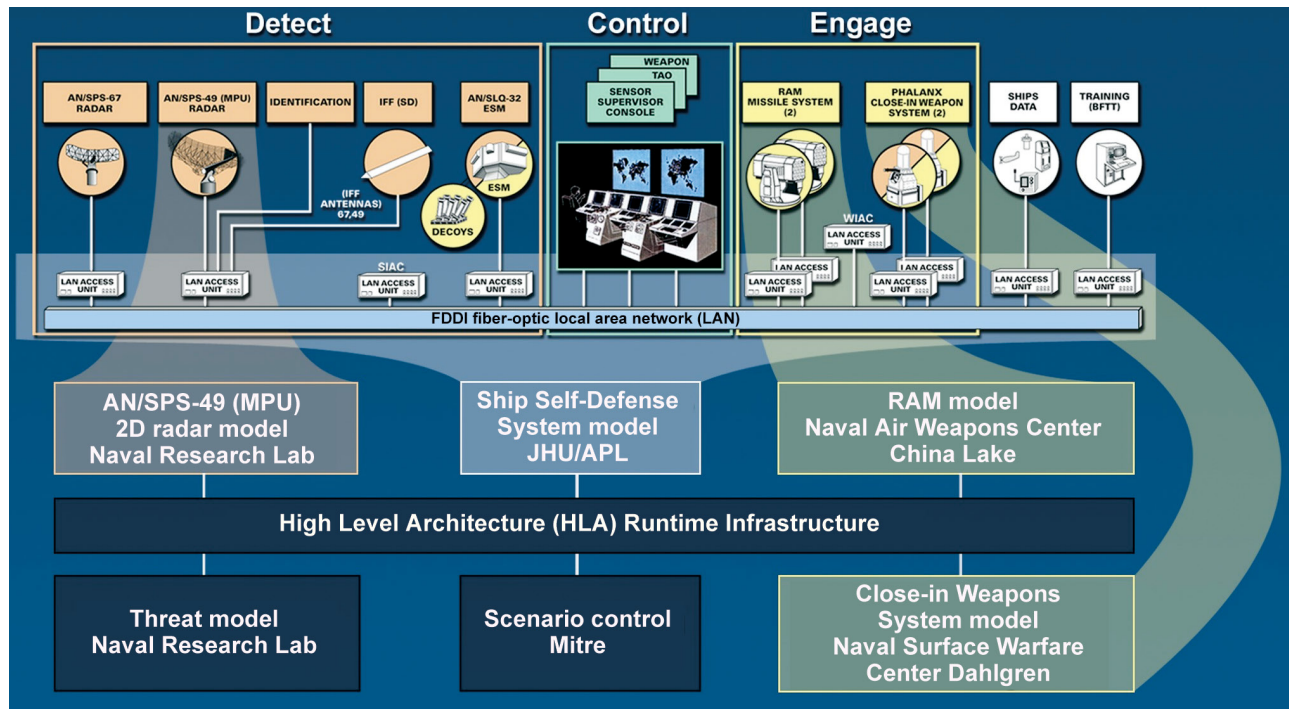
Figure 7. Integrated Ship Defense Advanced Distributed Simulation HLA pilot components (integrated ship defense high-fidelity simulation federation).

the AN/SPS-48E and AN/SPQ-9B surveillance radars currently used in PRA predictive analysis would be rehosted in a workstation of suitable speed and memory capacity to allow membership in an HLA federation. The other members of the federation would be a threat federate (e.g., based on the Naval Research Laboratory's CRUISE model), an own-ship federate, a scenario control federate, an electronic warfare federate such as AN/SLQ-32 or Advanced Integrated Electronic Warfare System, and an SSDS Mk 2 control system federate consisting of CEP Version 2.1 and SSDS Mk 2 software rehosted in a workstation. (A CEP 2.1 element is the front end of SSDS used to form composite tracks.) A federation of this scale would support detection and control aspects of PRA. Expanding the federation to include a RAM federate and electronic attack federate would round out the engagement aspects of PRA. Figure 8 shows a possible PRA federation as it applies to the detect, control, and engage segments of the analysis. All federates would interact via the RTI.

CONCLUSION

This article discussed several areas in which APL solved development and test challenges using various simulation capabilities. Simulators continue to provide a cost-effective alternative to the use of live assets as circumstances permit and will likely play even greater roles
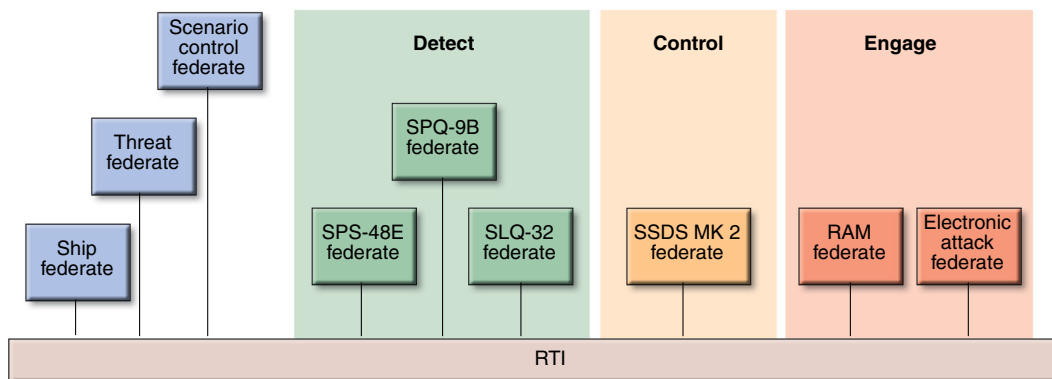

Figure 8. PRA federation.

in the future. The levels of integration being achieved in the battle space are placing ever-greater demands on the simulation tools, and APL is committed to pursuing the right solutions for these challenges. Accreditation of the simulators provides confidence to DoD acquisition agents when they are making decisions based on results of tests using those simulators. The recent WASP accreditation efforts have played an important role in helping the Navy reduce costs for the CEC program while maintaining confidence in its technical and programmatic decisions.

REFERENCES

[1]*IEEE Standard Glossary of Modeling and Simulation Terminology*, IEEE Standard 610.3-1989 (1989).
[2]*Department of Defense Modeling and Simulation (M&S) Master Plan*, DoD 5000.59-P (Oct 1995).
[3]*The Defense Acquisition System (Change 1)*, DoD Directive 5000.1 (23 Oct 2000).
[4]*DoD Modeling and Simulation Management (Change 1)*, DoD Directive 5000.59 (20 Jan 1998).
[5]*Accreditation of the CEP WASP for Developmental Testing and Evaluation, Independent Verification and Validation, and System Development*, PMS-465 Memorandum 9800 Ser 465 (Feb 2000).
[6]*Accreditation of the Cooperative Engagement Processor (CEP) Wrap Around Simulation Program (WASP) for Operational Evaluation (OPEVAL (OTIIA-4))*, PMS-465 Memorandum TSC ITF 9800 Ser TSC ITF/105 (27 Nov 2000).
[7]*Amended Accreditation of the Cooperative Engagement Processor Wrap Around Simulation Program for Operational Evaluation OTIIA-4*, PMS-465 Memorandum 5305 Ser 465/095 (11 Apr 2001).
[8]*IEEE Standard for Distributed Interactive Simulation*, IEEE Standard 1278.1-1995 (1995).
[9]McConnell, J. H., *The Navy Distributed Engineering Plant—Value Added for the Fleet*, Engineering the Total Ship 2002 Symp., Gaithersburg, MD (26–27 Feb 2002). Available at http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl (accessed 22 April 2002).
[10]*LPD 17 Probability of Raid Annihilation (PRA) Technical Approach*, NSWCDD/TR-00/58 (Aug 2000).
[11]*IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)—Framework and Rules*, IEEE Standard 1516-2000 (2000).

THE AUTHORS

BRUCE L. BALLARD is a member of APL's Senior Professional Staff. He received a B.S. in electrical engineering from the University of South Florida in 1984 and an M.S. in electrical engineering from The Johns Hopkins University Whiting School of Engineering in 1990. Mr. Ballard joined APL in 1985 and has experience in digital hardware design, communications, systems engineering, modeling and simulation, and real-time software development. Since 1996 he has been working on combat systems engineering and developing related real-time simulations for the Cooperative Engagement Capability and Ship Self-Defense System programs. Mr. Ballard is currently an Assistant Supervisor of the Battle Force Integration Group of the Air Defense Systems Department. His e-mail address is bruce.ballard@jhuapl.edu.

ROBERT E. ELWELL Jr. is a member of APL's Senior Staff and a Section Supervisor in the Air Defense System Department's Real-Time Systems Group. He received a B.S. degree in physics from Drexel University in 1985 and an M.S. degree in computer science from The George Washington University in 1990. Since joining APL in 1997, he has worked on sensor simulation programs used to develop and test the Ship Self-Defense System (SSDS) Mk 1 and Mk 2 programs, led an Independent Research and Development effort to identify issues associated with using High Level Architecture (HLA) in real-time simulations, and performed analysis to support the development of the Navy's Distributed Engineering Plant. Mr. Elwell currently is the SSDS Mk 2 Technical Direction Agent on-site representative at Raytheon Company in San Diego, CA. His e-mail address is robert.elwell@jhuapl.edu.
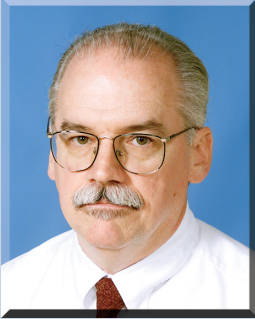
ROBIN C. GETTIER is a member of the Senior Professional Staff of the Air Defense Systems Department. He holds a B.A. in mathematics from Washington College. His work has been concentrated in the area of modeling and simulation at APL for systems such as AN/SYS-1, AN/SYS-2, RNSSMS, CEC, and SSDS. He is currently involved in modeling and simulation applications for probability of raid annihilation analysis. His e-mail address is robin.gettier@jhuapl.edu.

FRANCIS P. HORAN is a member of APL's Senior Staff. He is Supervisor of the Real-Time Simulation Integration Section of the Battle Force Integration Group of the Air Defense Systems Department. He specializes in real-time software and systems in Navy AAW applications. Mr. Horan received a B.S.E.E. from Drexel University in 1987 and an M.S.E.E. from The Johns Hopkins University in 1991. After joining APL in 1987, he was involved with real-time software development for the CEP, AutoID, and Dual Net MFL systems. Currently, he is active in real-time software development and system design of CEP HWIL testbeds. His e-mail address is fran.horan@jhuapl.edu.

ARTHUR F. KRUMMENOEHL is a member of APL's Principal Professional Staff and Assistant Supervisor of the Sensor and Weapon Control Engineering Branch of the Air Defense Systems Department. He has a B.S. in electrical engineering from Lehigh University and an M.S.E.E. in electrical engineering from the Massachusetts Institute of Technology. Mr. Krummenoehl has extensive experience in systems engineering and software development for radar detection and tracking systems, the Cooperative Engagement Capability, and the Ship Self-Defense System. He led development of wrap-around simulations used to test software-intensive systems. He has also led APL's work on the Ship Self-Defense pilot program and LPD 17 class Probability of Raid Annihilation assessment tool concept, and he was a member of the task forces for the Navy and Joint Distributed Engineering Plants. His e-mail address is arthur.krummenoehl@jhuapl.edu.

DAWN B. SCHEPLENG joined APL in 1987. She is currently an Assistant Supervisor of the Battle Force Integration Group in the Air Defense Systems Department. She received a B.S. in mathematical science from Loyola College in 1987 and an M.S. in computer science from The Johns Hopkins University in 1998. Ms. Schepleng initially worked on software development for various tactical shipboard systems and their testbeds. Since 1989, she has primarily been involved in system design, development, integration, and test of real-time simulation programs used both to test and demonstrate the Cooperative Engagement Capability program. Her interests are embedded system development, communications, and troubleshooting. Her e-mail address is dawn.schepleng@jhuapl.edu.