Systems-of-Systems Network Engineering

William G. Bath and Gregory A. Miller

The DoD is moving rapidly toward relying on a networked force to more effectively counter the enemy across nearly all mission areas. The future networked force is envisioned to interoperate across a heterogeneous set of networks and to have the capacity and performance to facilitate very pressing warfighting applications with large numbers of network nodes. The force will operate over shared communication and network resources that can be readily composed into an interoperable system-of-systems. The U.S. military's Integrated Fire Control (IFC) capability is envisioned as a networked system-of-systems that integrates ships, aircraft, and ground-based weapon systems to counter air and missile threats. In this article, we explore engineering an interoperable networked system-of-systems for IFC, with focus on the communication and networking environment. This exploration includes developing specifications for defining functional consistency and performance interactions between critical internal components of the systems, as well as identifying a process for defining and maturing the networked system-of-systems design in a cost-constrained environment.

INTRODUCTION

> [A] revolutionary increase in combat effects [can be achieved] by shifting the focus from specific platforms to a netted striking force. Netting geographically dispersed sensors and shooters into a coherent fighting force that can—almost instantaneously—observe, orient, decide, and then act in response to enemy actions will dramatically increase the capability of deployed commanders to rapidly target and strike. . . .
>
> —Admiral John B. Nathman,
> U.S. Fleet Forces Command (2005–2007)[1]

The DoD is moving ever more rapidly toward relying on a networked force to more effectively counter the enemy across nearly all mission areas. The concept of a networked force is not new to the U.S. military services (referred to here as the Services), which have operated across tactical data links for decades with networks such as Link-11 and Link-16. However, these networks do not provide the performance, the level of information access, or the interoperability envisioned as requirements for our future networked force. The potential for a significant increase in warfighting capability through fighting as a truly networked force was first discussed by APL researchers in detail in 1973.[2] The future networked force is envisioned to interoperate across a heterogeneous set of networks, to have the capacity and performance to facilitate very pressing warfighting applications with large numbers of network nodes, to operate over shared communication and network resources in support of multiple simultaneous missions, and to be readily composed into an interoperable system-of-systems. This article explores engineering a networked system-of-systems with Integrated Fire Control (IFC) as the mission application.

IFC: THE ENVISIONED SYSTEM-OF-SYSTEMS

The unique characteristic of IFC is the ability to execute engagements of targets by using the sensor or sensors best suited to track the target and by using the weapon or weapons most suited to killing the target without limitations imposed by "stovepiped" networks and software. In most cases today, weapon and sensor pairings are limited by constraints, such as that the sensor and weapon be located on the same platform, that they be directly connected on the same communications network, or that they were developed by the same military service or even the same program office within that service. Over the years, sensor–weapon pairs have been carefully engineered so that the control of the weapon is exactly matched to the sensor that normally supplies the data. Although this can produce a very high performance design, it can also make shooting the weapon on the basis of other sensor data impossible unless the supporting sensor data exactly corresponds to the sensor data one is used to working with. The concept of "any sensor, any shooter" dictates that the system-of-systems be designed so that, where physics will allow it, any weapon can be employed using data from any sensor. Meeting this condition requires engineering the many components of ship, air, and land weapon systems to be fully interoperable.

CRITICAL CHALLENGES

Critical challenges to be considered in engineering a networked system-of-systems include network and system performance, network security, and systems interoperability. Performance, security, and interoperability implementations will affect each other, and the overall performance of the system-of-systems must be considered during engineering and development. Additional considerations when engineering the networked system-of-systems are the use of existing and shared networking resources and the interoperability with existing operational systems. The Services typically cannot upgrade or replace existing networking infrastructure across the entire force or build standalone networks for each new networked system-of-systems, nor can they replace overnight the systems they currently have in place. This process often takes years, if not decades. There is no single or simple solution to these challenges. The networked system-of-systems must be engineered to accommodate the evolutionary nature of this upgrading and fielding process.

Unique Challenges for the IFC System-of-Systems

Engagements generally can be divided into three phases: (*i*) finding and identifying the target, (*ii*) making the engagement decision, and (*iii*) controlling the weapon. Each of these phases presents unique challenges for the IFC system-of-systems. Finding and identifying the target is dominated by the challenge of minimizing mistakes in the following areas: detection of targets that are not actually there, resulting in wasted engagements; the mistaken identification of a friendly or neutral target as hostile, resulting in potential loss of life of friendly or noncombatant forces; and the mistaken identification of a hostile target as friendly or neutral, resulting in a missed engagement opportunity. During the "finding and identifying" phase, one seeks to network sensors of vastly different modalities. During the "making the engagement decision" phase, one seeks to have the same track numbering system at all potential shooters so that the same physical object (e.g., aircraft or missile) is identified by the same track number on all units. During the "weapon control" phase, one seeks to have a very precise track of the target to make the weapon as effective as possible. These phases happen concurrently for many different weapon systems and targets.

To design interoperability into all the components, one must analyze and specify component performance at multiple levels (Fig. 1). At the first level, one has overall expectations of the performance of the system-of-systems as judged by warfighting metrics such as probability of raid annihilation, effective operating areas, etc. At the final level (level 6 in Fig. 1), one has the actual realized performance of these metrics. In between the first and last levels, one specifies the interaction of the components to ensure this performance. The top-level specification (level 2 in Fig. 1) includes

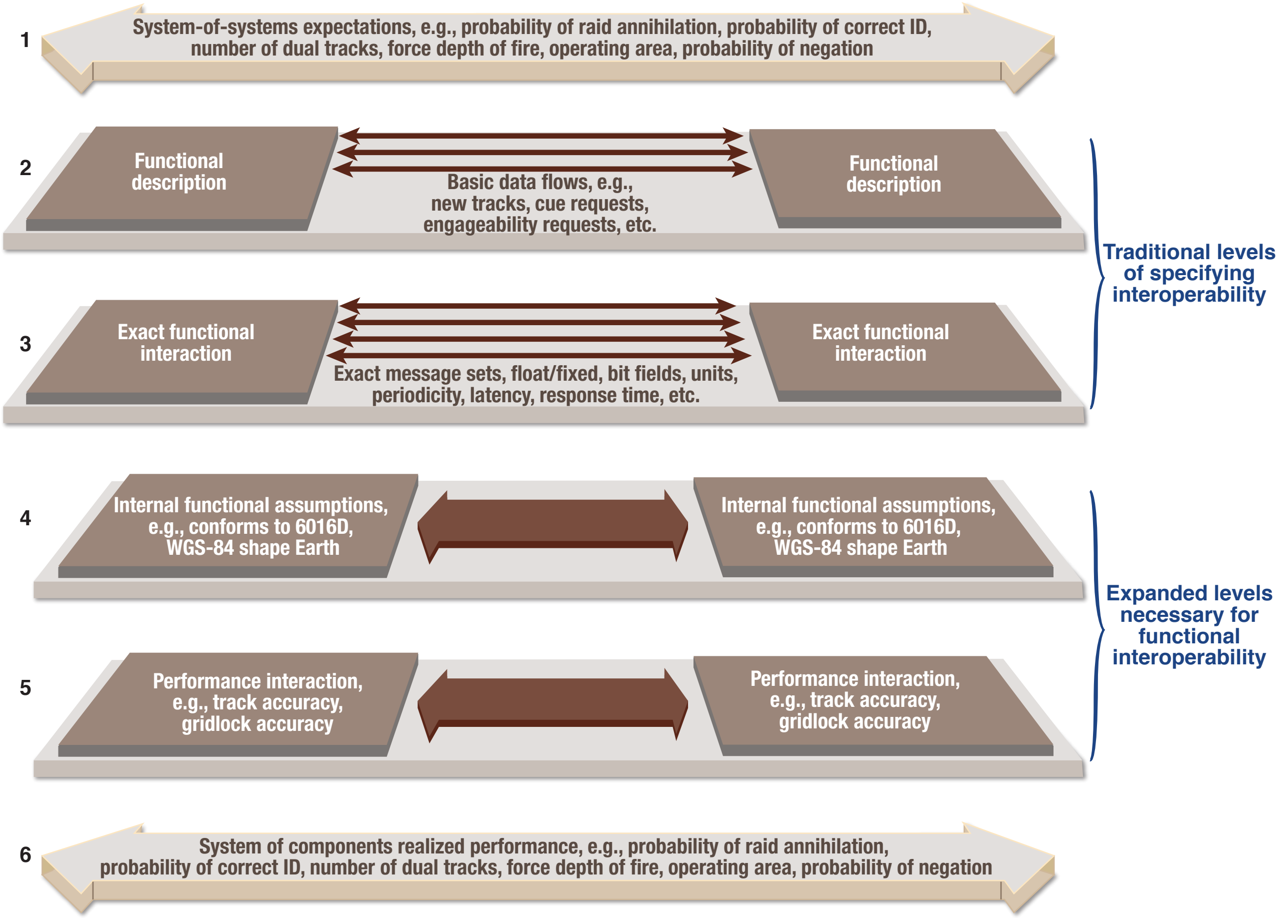

1
System-of-systems expectations, e.g., probability of raid annihilation, probability of correct ID, number of dual tracks, force depth of fire, operating area, probability of negation
2
Functional description
Basic data flows, e.g., new tracks, cue requests, engageability requests, etc.
Functional description
3
Exact functional interaction
Exact message sets, float/fixed, bit fields, units, periodicity, latency, response time, etc.
Exact functional interaction
Traditional levels of specifying interoperability
4
Internal functional assumptions, e.g., conforms to 6016D, WGS-84 shape Earth
Internal functional assumptions, e.g., conforms to 6016D, WGS-84 shape Earth
5
Performance interaction, e.g., track accuracy, gridlock accuracy
Performance interaction, e.g., track accuracy, gridlock accuracy
Expanded levels necessary for functional interoperability
6
System of components realized performance, e.g., probability of raid annihilation, probability of correct ID, number of dual tracks, force depth of fire, operating area, probability of negation

Figure 1. To realize the desired performance of the system-of-systems, the interaction between components must be specified not just at the traditional levels—basic data flows and exact functional interaction—but also at the levels of internal functional assumptions and performance interaction. WGS-84, World Geodetic System 1984.

basic data flows (tracking messages and engagement control messages). This specification ensures that every critical path exists and every need for data is satisfied, at least conceptually. The next level (level 3 in Fig. 1) defines the exact functional interaction to the bit level, making sure that data types, latencies, and response times meet the need. But these traditional levels of specifying interfaces are insufficient for true interoperability at the functional level. Two additional levels are needed if components are to interoperate not just in a computer science sense but also in a warfighting sense. The internal functional assumptions (level 4 in Fig. 1) must be specified to be consistent. Defining specifications for internal functional assumptions ensures that the basic engineering parameters used in the components are consistent. The performance interaction (level 5 in Fig. 1) must also be specified. Defining specifications for performance interaction ensures that the quantitative performance (e.g., accuracy, dynamic response, stability) of each component is compatible with the other components.

NETWORKING ENVIRONMENT

The DoD's vision is to move toward a networked force with a ubiquitous, globally interconnected warfighting capability much like the capability for interconnection the World Wide Web provides us in our daily lives. This vision is being pursued with significant investment by the DoD under the guise of the Global Information Grid (GIG). As originally envisioned, the GIG would ultimately interconnect sensors, weapon systems, command and control systems, and warfighters and would provide seamless access to information based on the need and security level of the user. Realization of this ubiquitous capability is many decades away. For many of the military's real-time tactical applications, however, it is much closer, and it can be realized for applications with less stringent real-time performance requirements. As we engineer new networked systems-of-systems and evolve toward the networked force, we must keep the long-term vision in focus and in perspective to meet system performance objectives. It is likely that performance, security, and interoperability with legacy systems will drive near- and mid-term solutions toward a hybrid of closed and legacy network environments and GIG-like environments for many networked systems-of-systems.

Networking Environment for the IFC System-of-Systems

The networking environment for IFC is dominated by the mobile nature of the ships, aircraft, and land forces. In office and home Internet-based networks, the basic electrical connectivity is provided by relatively reliable and inexpensive media—coaxial or fiber optic cables. In contrast, IFC networks require exchange of large amounts of very timely data over terrestrial radio networks. These radio networks must be designed to meet time latency, reliability, throughput, and antijam/antifade performance expectations. The principal drivers in achieving these objectives are the basic RF parameters of transmitter power and antenna gain, which determine how much power a radio will receive. In addition, low antenna sidelobes and a wide RF operating band make the radio far less susceptible to jamming. Agility provides robustness in the environment and is essential both to the connections that are used for routing and across the frequency spectrum. Finally, the mobile nature of the problem leads to rapidly changing network topologies and routings. This changing environment requires data to be selected and prioritized to fit through occasional routing bottlenecks, and it requires the ability to form and modify networks "on the fly" in a matter of seconds. Table 1 illustrates the impact of radio network design features and the corresponding quality of service primarily impacted.

DEVELOPING AND MATURING AN INTEROPERABLE SYSTEM-OF-SYSTEMS

It is instructive to consider successful developments of complex systems-of-systems. Figure 2 illustrates three such developments: the Aegis Weapon System, the Cooperative Engagement Capability (CEC), and Aegis Ballistic Missile Defense. All three are complex systems having several complex subsystems whose designs are very dependent on each other and whose individual and integrated performance is dependent on the physics of both the natural and the threat environment. In addition, all three have many outside interfaces to other systems (whose designs are largely beyond their control) that can materially affect their performance. In each case, a conscious decision was made that the community's understanding of the problem and technical knowledge of how to solve it were insufficient at the start of the program to proceed directly to a production solution.

Accordingly, each program spent about 10 years in an interactive develop–test–learn cycle. The USS *Norton Sound*, a World War II seaplane tender, was modified to carry the first Aegis development model. Extensive tests of the new phased-array radar, of nascent software control processes, and of the Standard missile and missile launching system were conducted in a maritime environment. Significant changes were made to the designs of the radar signal processing, the electronic countermeasures, and the weapon control software. CEC evolved from a network of similar sensors terminating in a display in the combat system in 1990 to a much more tightly integrated system of more diverse sensors in 2001, capable of supporting fire control and of interoperating

Table 1. Radio network design characteristics are primary drivers determining the quality of service for the IFC system-of-systems

	Quality Factors			
Characteristic	Time Latency	Reliability	Throughput	Antijam/Antifade
Transmitter power		✓	✓	✓
Antenna gain		✓	✓	✓
Antenna sidelobes				✓
RF operating bandwidth		✓	✓	✓
Agility				
• Connections	✓			
• Frequency		✓		✓
Network control automation				
• Data selection/priority	✓		✓	
• Routing	✓	✓	✓	✓
• Transmission scheduling	✓		✓	

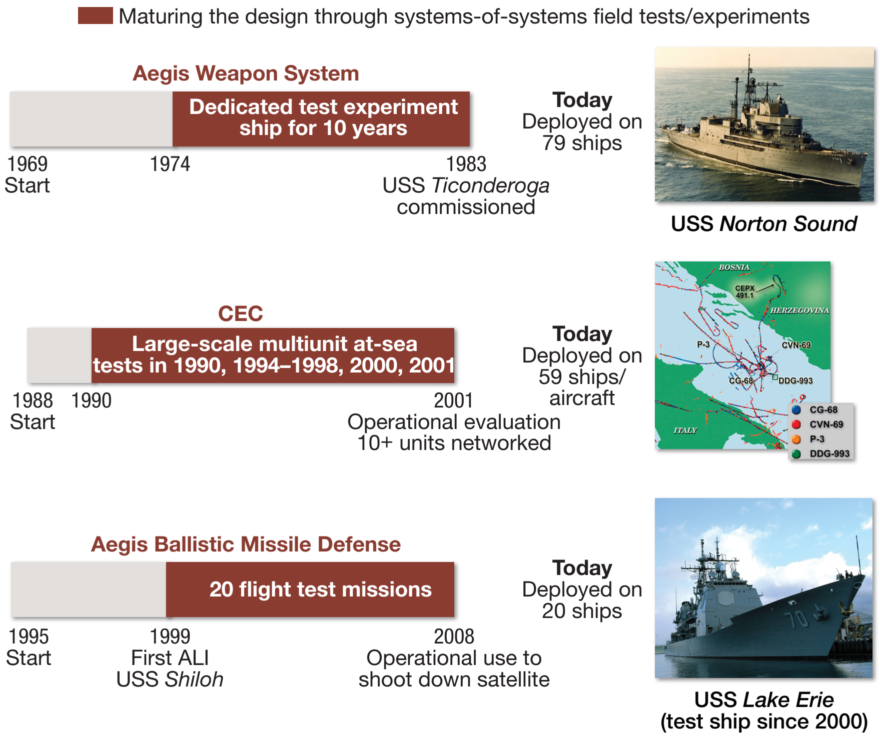

Maturing the design through systems-of-systems field tests/experiments
Aegis Weapon System
Dedicated test experiment ship for 10 years
1969 Start
1974
1983 USS Ticonderoga commissioned
Today Deployed on 79 ships
USS Norton Sound
CEC
Large-scale multiunit at-sea tests in 1990, 1994–1998, 2000, 2001
1988 Start
1990
2001 Operational evaluation 10+ units networked
Today Deployed on 59 ships/ aircraft
BOSNIA
CEPX 491.1
HERZEGOVINA
P-3
CVN-69
CG-68
DDG-993
ITALY
CG-68
CVN-69
P-3
DDG-993
Aegis Ballistic Missile Defense
20 flight test missions
1995 Start
1999 First ALI USS Shiloh
2008 Operational use to shoot down satellite
Today Deployed on 20 ships
USS Lake Erie (test ship since 2000)

Figure 2. Examples of three complex systems-of-systems, each of which was matured through approximately 10 years of extensive, critical experiments in the field. CEPX, Cooperative Engagement Processor Track Number Index; CG-68, guided missile cruiser 68; CVN-69, Nuclear Powered Aircraft Carrier 69; DDG-993, Guided Missile Destroyer 993; P-3, P-3 Orion aircraft.

with other networks.[3] Aegis Ballistic Missile Defense introduced an entirely new, hit-to-kill weapon type into the Navy. This concept was prototyped during the first Aegis Lightweight Exoatmospheric Projectile (LEAP) Intercept (ALI). The integration of the eventual Standard Missile-3 missile elements with sensors and combat system elements was matured over a series of 20 flight-test missions over a 10-year period.

Regardless of the acquisition strategy pursued, the design maturation period is essential. (Interestingly, this period was about 10 years for each of these complex system-of-systems examples.) A system-of-systems development process should mature the design throughout the development process, as shown in Fig. 3. This maturation should occur during (not after) the development process, because during development is when the program funding and momentum are available to accomplish it. The three examples cited above all used extensive field testing to mature the design. This is clearly the preferred approach; however, fiscal realities have opened the question of how much field testing can be replaced by laboratory modeling and simulation.

The goal of a modeling and simulation-based design maturation process would be to replace the 10-year field test period with a mix of modeling, simulation, and field testing to deliver the mature system-of-systems within fiscal constraints (Fig. 4). The remainder of this article discusses how this might be done.

Without a design maturation phase occurring simultaneously with the system development, performance of the system-of-systems is totally dependent on the understanding of the process at the beginning of development, as captured in design specifications, interface specifications, and statements of work. The understand-

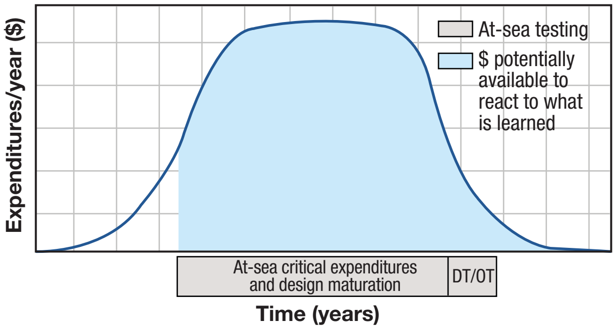


Figure 3. The three examples described in Fig. 2 all included extensive field testing to mature the design. This maturation occurred simultaneously with development. DT/OT, development test/operational test.

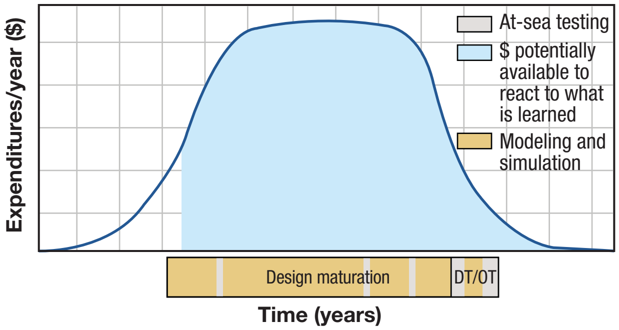


Figure 4. The goal is to use modeling and simulation as the primary methodology, with at-sea testing at critical junctures, to mature the system-of-systems.

ing captured at this stage is seldom deep and detailed enough, nor captured far enough in advance, to ensure that the final system-of-systems will be interoperable and effective. DoD acquisition history, unfortunately, contains many examples of developments that reached the end of the development (and funding) cycle without ever being matured to the point at which they could be deployed.

The activities needed to mature a complex system-of-systems design can be characterized by two types of experimental fidelity: physics fidelity and tactical system content. These are plotted as a two-dimensional grid in Fig. 5. The ordinate—physics fidelity—ranges from simple cookie-cutter models, to effects-based models, to high-fidelity models with precise modeling of the physics of the natural and threat environment, to replay of collected signals from field data, to actual tests in the field (this last being the epitome of physics fidelity). The abscissa—tactical system content—recognizes the complexity of human-made systems. It ranges from predictive models, to mixtures of predictive models and parts of real systems, to real tactical hardware and software. The lower-left quadrant of Fig. 5 shows the use of models of potentially wide scope but having very simple representations of the physics of sensors and weapons and having little tactical content (e.g., no embedded tactical software). These models are better suited to top-level requirements definitions and campaign analyses than to design and development. The upper-left quadrant shows the high modeling fidelity, possibly supplemented with field testing, but the tactical system content is low. Here one learns about algorithms, signal characteristics, and environmental factors that are essential to the design, but such modeling does not consider exactly how the many subsystems have been or are being built. The lower-right quadrant shows actual tactical hardware and software components that are integrated and tested, but the physics of the environment is absent. Finally, the upper-right quadrant combines both high physics fidelity and high tactical system content. This type of modeling can be accomplished by taking the built system or a built system prototype into the field or into a sophisticated test fixture that can replicate the physics of the real world.

Despite the great success achieved through extensive critical experiments, many new acquisition programs today skip this step in the interest of reducing cost. This approach produces a process-oriented system-of-systems design maturation shown in Fig. 6. Here one operates in the upper-left quadrant of simultaneous high physics fidelity and high tactical system content only at the end of the development, once the components have been fully developed. The huge disadvantage to this approach is that individual component designs (each one potentially being an effort costing tens to hundreds of millions of dollars) can proceed to completion before it is learned that a different design approach is needed for successful interoperability with the other components.

Based on the three successful developments described at the beginning of this section, the lower-risk (and eventually lower-cost) approach is to continually reevaluate component functions and performance through a series of critical experiments proceeding in parallel with the development efforts (Fig. 7).

Closing the Gaps in Developing and Maturing an Interoperable IFC System-of-Systems

In the past, successful, complex systems-of-systems have been developed with extensive prototyping by using a philosophy of “build a little, test a little.” This approach has matured the design of the networks, the applications interacting over the networks, and the overall performance of the weapon system. The challenge is determining how to follow this approach in a budget-constrained environment. Two key gaps exist in our current ability to do so.

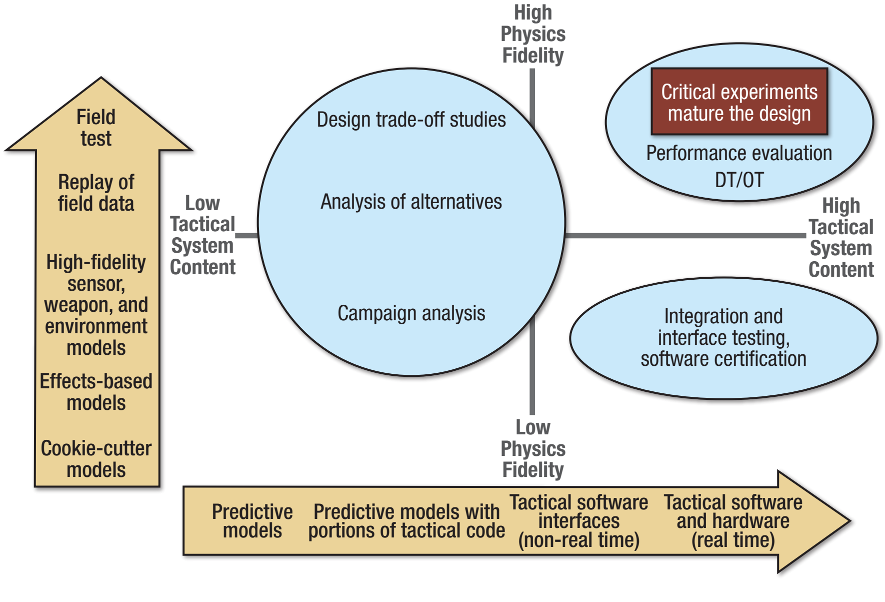

High Physics Fidelity
Field test
Replay of field data
High-fidelity sensor, weapon, and environment models
Effects-based models
Cookie-cutter models
Low Tactical System Content
Design trade-off studies
Analysis of alternatives
Campaign analysis
Critical experiments mature the design
Performance evaluation DT/OT
High Tactical System Content
Integration and interface testing, software certification
Low Physics Fidelity
Predictive models
Predictive models with portions of tactical code
Tactical software interfaces (non-real time)
Tactical software and hardware (real time)

Figure 5. The activities needed to mature a complex system-of-systems design can be plotted as a two-dimensional grid of physics fidelity versus tactical system content.

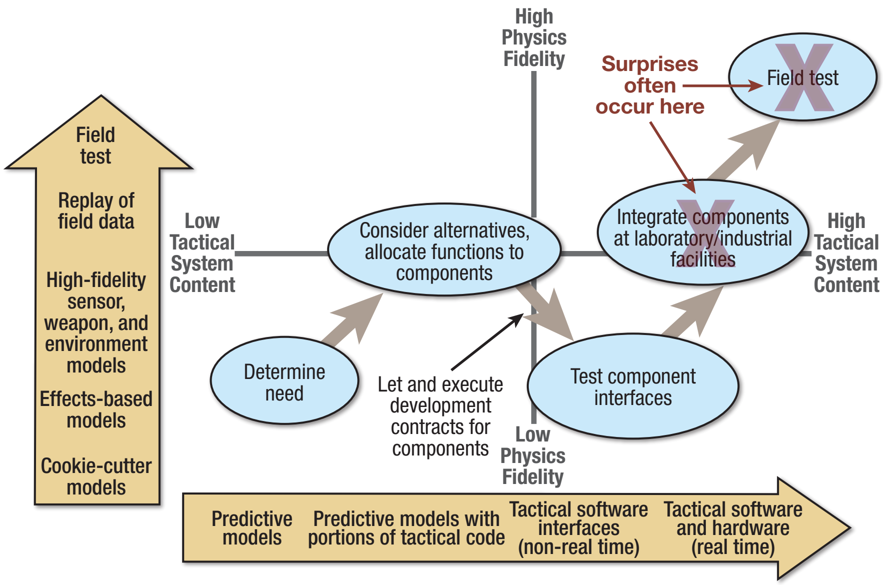

High Physics Fidelity
Surprises often occur here
Field test
Field test
Replay of field data
High-fidelity sensor, weapon, and environment models
Effects-based models
Cookie-cutter models
Low Tactical System Content
Consider alternatives, allocate functions to components
Integrate components at laboratory/industrial facilities
High Tactical System Content
Determine need
Let and execute development contracts for components
Test component interfaces
Low Physics Fidelity
Predictive models
Predictive models with portions of tactical code
Tactical software interfaces (non-real time)
Tactical software and hardware (real time)

Figure 6. A process-oriented system-of-systems design maturation approach can lead to unpleasant surprises during integration and field testing, when components may need to be redesigned to achieve interoperability.

The first gap is in the ability to do predictive modeling of the system-of-systems. Figure 8 compares development approaches for missiles, radars, and system-of-systems interoperability. An essential step is the ability to model alternative approaches and predict performance before full-scale production. In designing a missile system, one answers basic architectural questions (e.g., active or semiactive guidance? proportional navigation?) through modeling and simulation prior to full-scale development. The same is true for radar design, in which basic decisions about frequency band, antenna design, beamforming, and waveforms must be made before full-scale development. For missiles, the modeling standard at APL is a 6-degree-of-freedom (6DOF) simulation.[4] For radars, there are a variety of predictive analysis approaches, but the FirmTrack model is APL's preferred approach. However, as shown in Fig. 8, there is no modeling standard for system-of-systems interoperability. APL is addressing this gap through an Independent Research and Development effort, the Componentized Combat System Analysis Framework, which is using new technology to incorporate models into federations with little or no change to the model and to run system-of-systems federations at much higher speed than previous federations, facilitating Monte-Carlo analysis (Miller, A. J., and Kahn, S. A., "A Faster Than Real-Time Simulation Framework," presented at Modeling and Simulation in Test and Evaluation, Technical Exchange Workshop, Port Hueneme, CA, 2010).

The second key gap is in evaluating the effectiveness and interoperability of systems-of-systems as they are built, effectively maturing the designs during and after full-scale development. Historically, successful developments have accomplished this with extensive field testing. Although field testing is still the preferred approach, it is likely to be unaffordable in today's environment. An interesting case study (Fig. 9) was done by Bruce Ballard of APL (personal communication, 2007). In this study, the system-of-systems flaws found during

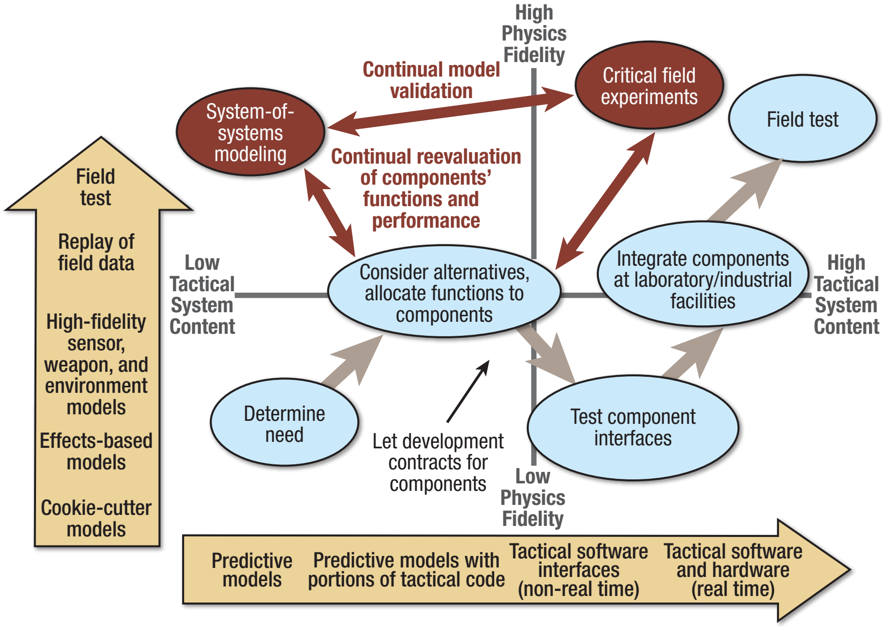

High Physics Fidelity
Continual model validation
Critical field experiments
Field test
System-of-systems modeling
Continual reevaluation of components' functions and performance
Field test
Replay of field data
High-fidelity sensor, weapon, and environment models
Effects-based models
Cookie-cutter models
Low Tactical System Content
Consider alternatives, allocate functions to components
Integrate components at laboratory/industrial facilities
High Tactical System Content
Determine need
Let development contracts for components
Test component interfaces
Low Physics Fidelity
Predictive models
Predictive models with portions of tactical code
Tactical software interfaces (non-real time)
Tactical software and hardware (real time)

Figure 7. Ongoing evaluations of critical functions and performance through modeling and simulation and critical experiments, in parallel with system development, will typically be a lower-risk and lower-cost approach to development of the system-of-systems.

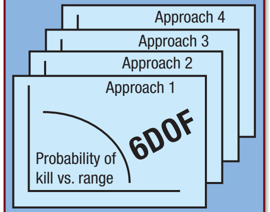
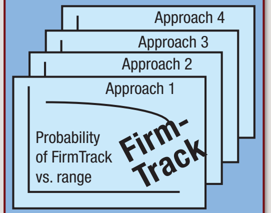
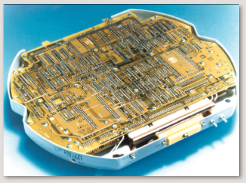
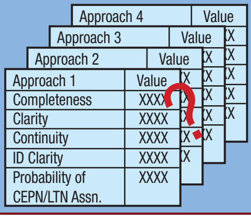
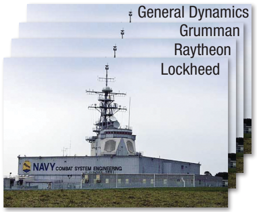
	Assess Gaps in Current Performance	Model Alternative Approaches and Predict Performance	Full-Scale Development	Integrate, Test, and Evaluate
Missiles	• Predictive analysis in approved scenarios • Fleet missile firings • Combat system ship qualification trials	 Approach 4 Approach 3 Approach 2 Approach 1 Probability of kill vs. range 6DOF		• Factory acceptance • White Sands • At-sea test
Radars	• Predictive analysis in approved scenarios • Tracking exercises • Deployed unit performance	 Approach 4 Approach 3 Approach 2 Approach 1 Probability of FirmTrack vs. range Firm-Track		• Factory acceptance • Land-based test site (e.g., Wallops/Patuxent Naval Air Station) • At-sea test
Interoperability	• Fleet training exercises • Distributed engineering plant (DEP) events	 Approach 4 Value Approach 3 Value Approach 2 Value Approach 1 Value Completeness XXXX Clarity XXXX Continuity XXXX ID Clarity XXXX Probability of CEPN/LTN Assn. XXXX ?	 General Dynamics Grumman Raytheon Lockheed NAVY COMBAT SYSTEM ENGINEERING	• Single unit (e.g., combat systems engineering development site) • Multiunit (Wallops, DEP) • At-sea test

Figure 8. Comparison of development phases for missiles, radars, and system-of-systems interoperability. Note today's lack of a way to model alternative approaches and predict performance for interoperability of systems-of-systems. APL is addressing this gap through the Componentized Combat System Analysis Framework Independent Research and Development project.

extensive at-sea testing of CEC were examined to determine how many could have been found in a modeling and simulation environment. Several hundred design flaws were considered individually and were classified. Approximately 63% of the design flaws were judged to be such that they could have been found in the laboratory; 21% were judged to require field testing. The rest were unclassifiable given the information available. This sort of result gives hope that the cost of system-of-systems design maturation can be reduced from that of the traditional model. However, a long way remains to ascertain how to make that cost reduction—that is, how to determine in advance which 63% of the field testing does not need to be done.

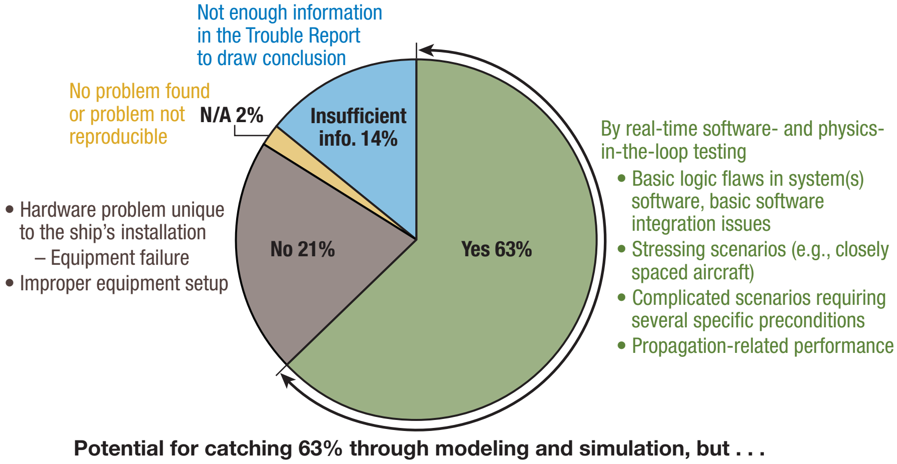


Figure 9. A case study of system-of-systems flaws found during extensive at-sea testing of CEC shows that a significant fraction of these flaws could have been found by software- and physics-in-the-loop testing, rather than by field testing.

SUMMARY AND CONCLUSIONS

In this article, we discussed engineering a complex networked system-of-systems for a tactical military mission capability, IFC, in terms of system-of-systems interoperability, networking, and development and maturation.

Interoperability

Engineering an interoperable system-of-systems that meets mission performance expectations for a complex mission capability such as IFC requires that traditional approaches for specifying interactions between systems, such as message exchanges and functional interactions, be expanded to include specifications for defining functional consistency between critical internal components of the systems and performance interactions for those internal system components that affect the capability of the system-of-systems.

Networking

Operational environments and system-of-systems performance requirements are key drivers to the network environment used for implementation of a system-of-systems. IFC networks require high-volume, timely, and reliable data exchanges between mobile air, ground, and sea surface platforms over terrestrial radio systems. Radio system design and performance will be the principal factor for achieving network performance for the IFC mission.

Development and Maturation

Experience has shown that a significant design maturation period is essential to the development and maturation of complex systems-of-systems for military applications, and that the designs for successfully fielded systems have typically matured simultaneously throughout the development process. A proven approach to maturing the design is continual evaluation of component functions and performance through extensive prototyping and critical experimentation that integrates both high-fidelity physics-based representations of the operating environment and high-fidelity tactical system content. The challenge faced in development of the IFC capability and other complex networked systems-of-systems is to accomplish a comparable level of maturation in a budget-constrained environment where the same level of prototyping and experimentation is not affordable. Modeling and simulation promises to help reduce that cost of the design maturation process; however, how much cost saving can be achieved is still to be determined.

The System-of-Systems Development Loop

Much like a missile or radar development, the IFC system-of-systems requires a disciplined development process (Fig. 10). APL has a unique collection of competencies for this problem: in the individual systems, in analysis of system requirements and interactions, and in the modeling and simulation technology necessary to model alternative approaches and predict performance for system-of-systems interoperability.

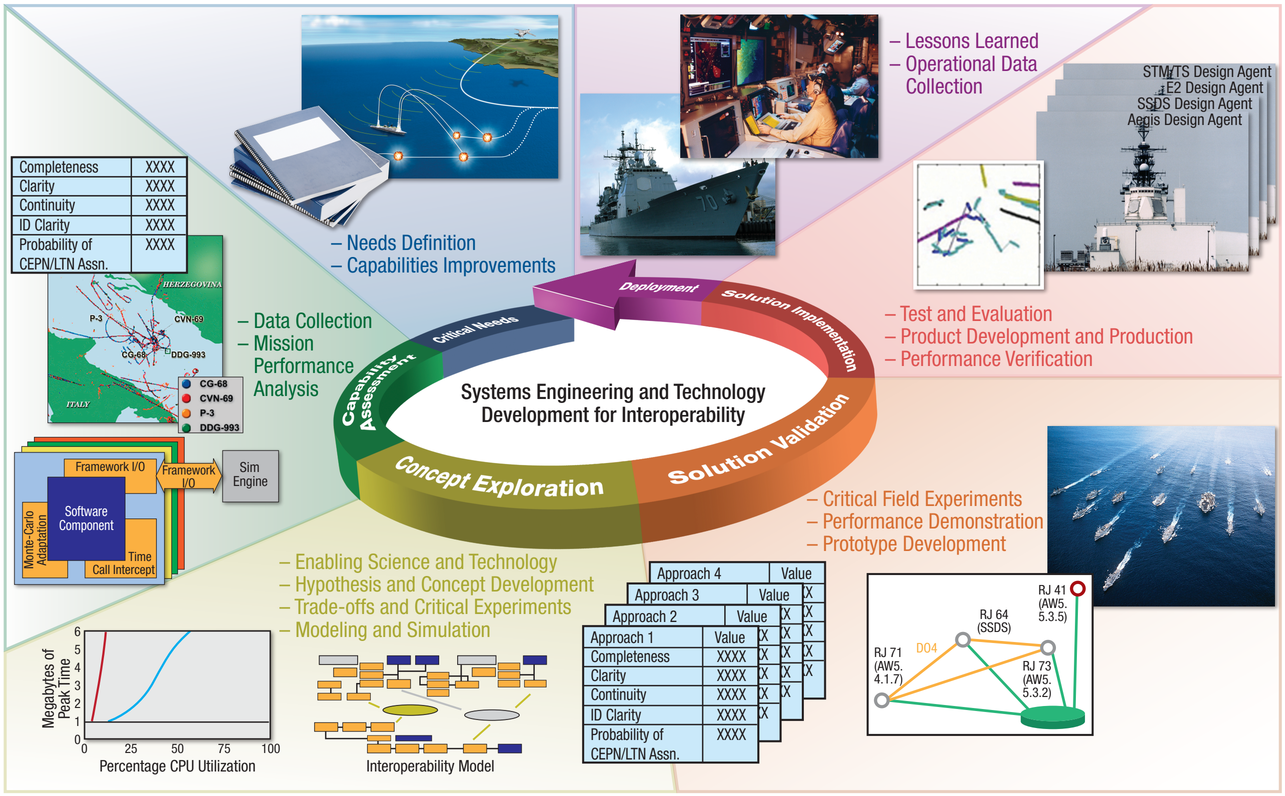


Figure 10. Developing and fielding an effective and interoperable IFC system-of-systems will require a "systems" approach to the networked system-of-systems.

REFERENCES

[1] Nathman, J. B., "A Revolution in Strike Warfare," *SEAPOWER*, Oct 1999, pp. 28–31.

[2] Eaton, A. R., "What Does Technology Offer?" in *Proc. Joint AIAA-AOA Tactical Missiles Meeting,* Orlando, FL, pp. 1–7 (1973).

[3] Krill, J. A., "Systems Engineering of Air and Missile Defenses," *Johns Hopkins APL Tech. Dig.* **22**(3), 220–233 (2001).

[4] Kuehne, B. A., Patterson, R. A., Schmiedeskamp, J. E., Harrison, G. A., Antonicelli, M. E., et al., "Standard Missile-2 Block IVA Analysis and Test," *Johns Hopkins APL Tech. Dig.* **22**(3), 248–259 (2001).

The Authors

William G. Bath

Gregory A. Miller

The system-of-systems networking teams in APL's Air and Missile Defense Department (AMDD) include more than 100 staff members working on tactical data links (Link-11 and -16) and the systems they interconnect (Aegis, Ship Self-Defense System, E-2C/D aircraft, and joint players such as the Army, Air Force, Marine Corps, and allies), CEC, and functions that require networking (anti-air warfare, ballistic missile defense, and IFC). **William G. (Jerry) Bath** has worked in this area for more than 30 years (spanning development of the Surface Gridlock System for Link-11 in the 1970s, CEC in the 1990s, and current work on interoperability of multiple networks). He supervises AMDD's Combat Systems Branch. For more than 22 years **Gregory A. Miller** has worked in the development of command and control capabilities and the integration of these capabilities from individual Navy platforms into an integrated battle force. He is currently the Program Area Manager for AMDD's Integrated Warfare System and Technologies program area. For further information on the work reported here, contact Jerry Bath. His e-mail address is william.bath@jhuapl.edu.

The *Johns Hopkins APL Technical Digest* can be accessed electronically at **www.jhuapl.edu/techdigest**.