Operational Testing of Defense Acquisition Programs in a System of Systems Environment

Catherine Warner, Science Advisor
Director, Operational Test and Evaluation

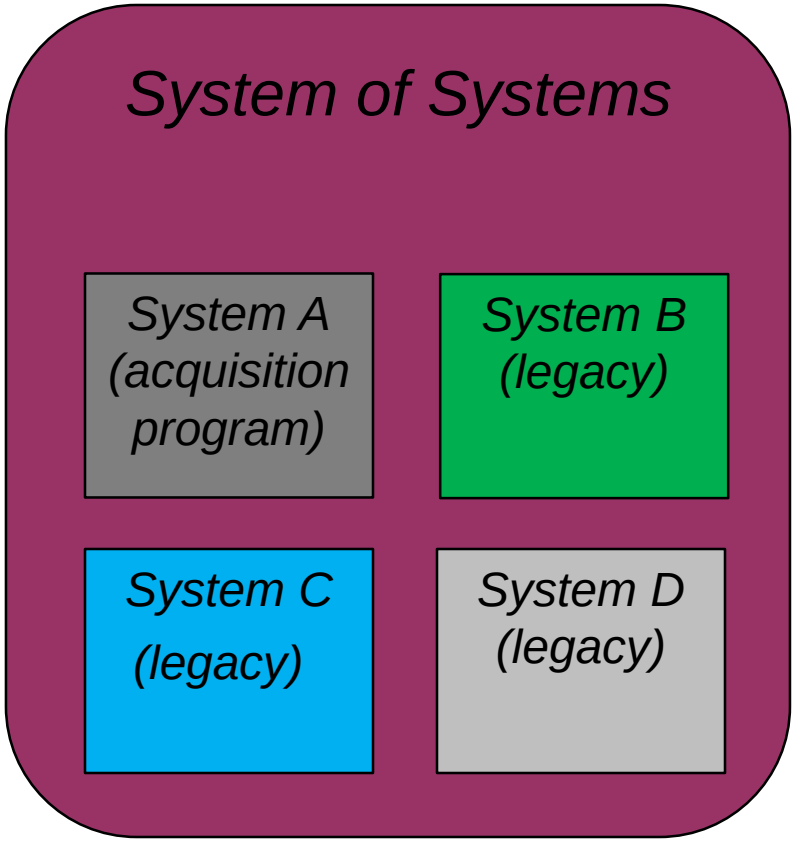
2016 System-of-Systems Engineering Workshop
International Test and Evaluation Association
January 28, 2016

Overview

- **Introduction**
- **How do we test a system in a SoS?**
- **Test Constructs and Examples**
- **Resolving Risk in 2020**

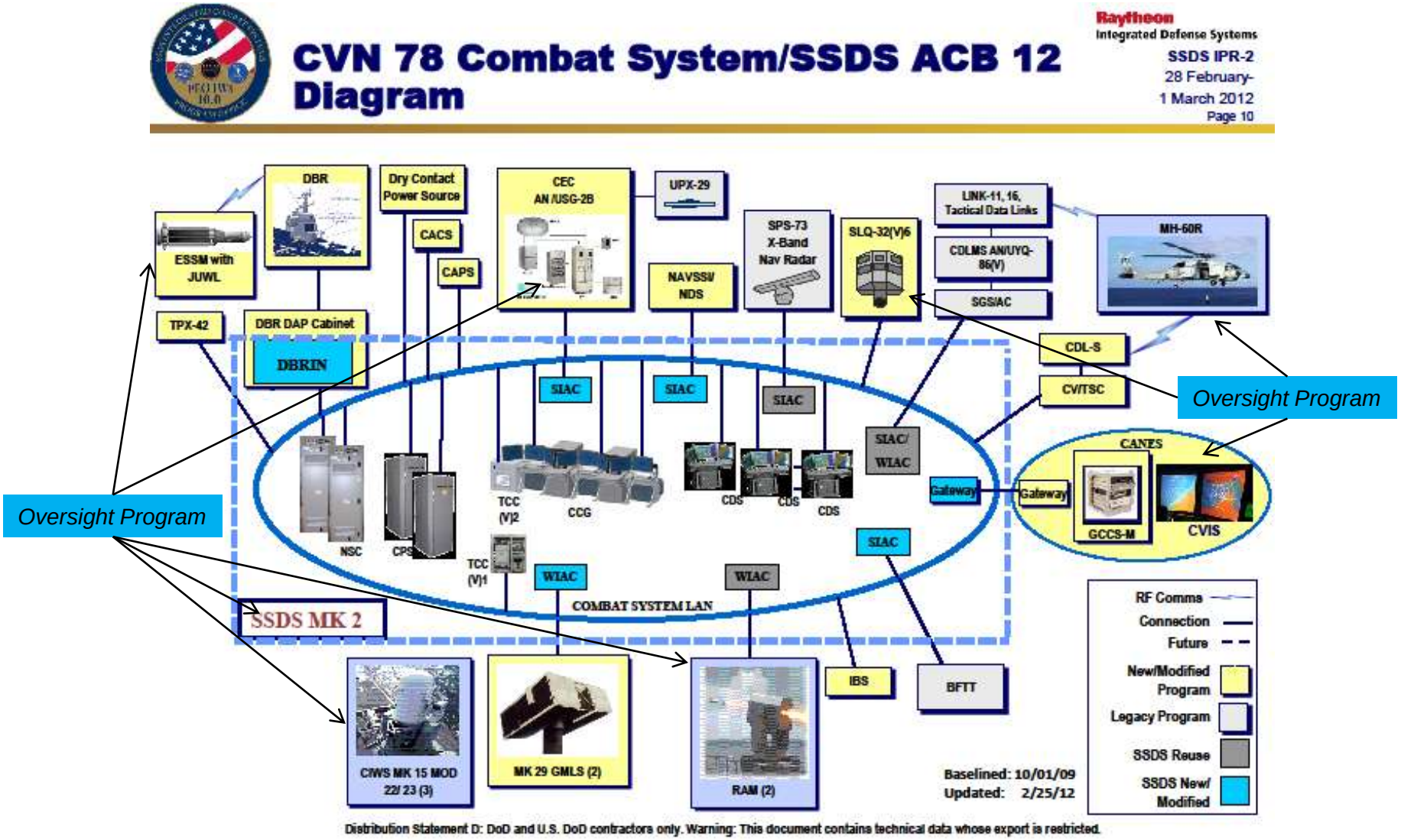
What is a System of Systems? (SoS)

- **Major defense acquisition programs are systems that are intended to operate in the context of a larger SoS**
- **Requirements are written for individual systems but do not specify the requirements of the SoS**
- **Operational testing requires the system operate in the SoS context, so that its ability to support the overall mission can be assessed**



"It's all about the Mission"

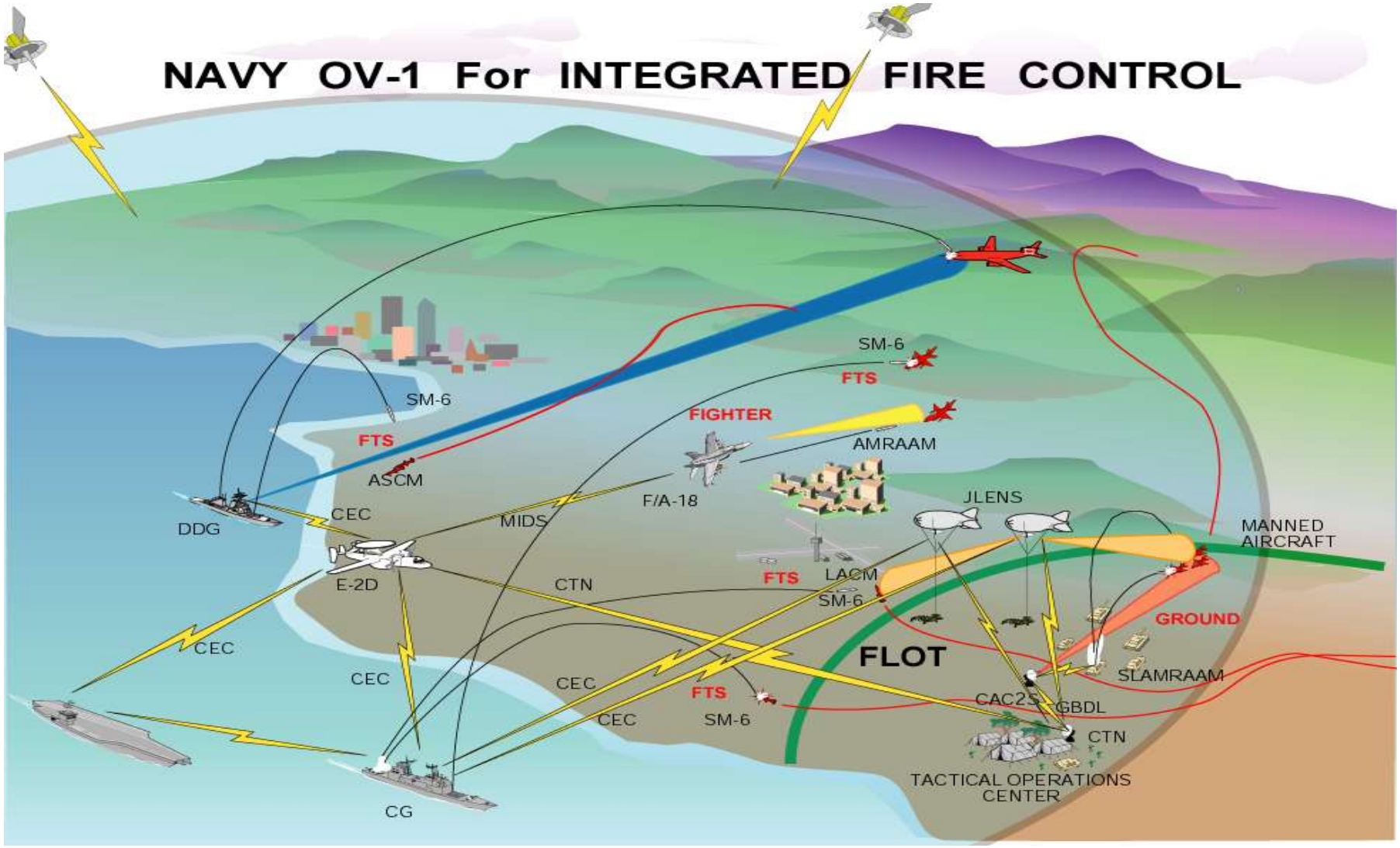
Example – Ship Combat Systems



Oversight Program

Oversight Program

Example – Naval Integrated Fire Control - Counter Air



Outline

- **Introduction**
- **How do we test a system in a SoS**
- **Test Constructs and Examples**
- **Resolving Risk in 2020**

Designing Operational Tests in a System of Systems Context

- **Operational testing requires that the acquisition program be tested in a realistic operational environment (i.e., in a SoS context)**

- **Focus on mission success for the SoS**
  - Does the new capability provided by the system under test support mission accomplishment for the SoS
    - » Develop metrics that measure mission success for the SoS
    - » Determine what data are necessary for the mission success metrics
    - » Develop test scenarios that provide the requisite data
  - Does the system meet its specified system requirements
    - » Use DT data to measure DT-like metrics
    - » CDD or CPD requirements are often insufficient for measuring mission success

- **When constructing SoS tests, try to satisfy both SoS T&E requirements and element system(s) T&E requirements**

Designing Operational Tests in a System of Systems Context (cont.)

- **An Enterprise approach is often useful to coordinate SoS testing across different programs**
  - This ensures that all programs that are needed for an adequate operational test participate.
- **If M&S is used for operational testing, the M&S needs to model the SoS (including the mission environment)**
- **Threat surrogates need to be validated and accredited at the SoS level and at the element level**
  - This increases the need to develop high fidelity threat surrogates

"It's all about the Mission"

Outline

- **Introduction**
- **How do we test a system in a SoS**
- **Test Constructs and Examples**
- **Resolving Risk in 2020**

Example - Ship Self Defense against Anti-Ship Cruise Missiles (ASCMs)

- **Background:**
  - USS *Stark* hit by two Iraqi Exocet ASCMs (1987)
  - Chief of Naval Operations defined self defense requirements for all current and planned ship classes.
  - The requirement is known as the Probability of Raid Annihilation (P_{RA}) requirement.
  - USS *San Antonio* (LPD 17) was the first ship class tested for the CNO's requirement.

- **Other ship classes that must demonstrate P_{RA} include the following:**
  - USS *America* (LHA 6) amphibious assault ship
  - USS *Zumwalt* (DDG 1000) destroyer
  - USS *Freedom* (LCS 1) and *Independence* (LCS 2) littoral combat ships
  - USS *Gerald R. Ford* (CVN 78) aircraft carrier
  - USS *Arleigh Burke* (DDG 51) Flight III guided missile destroyer

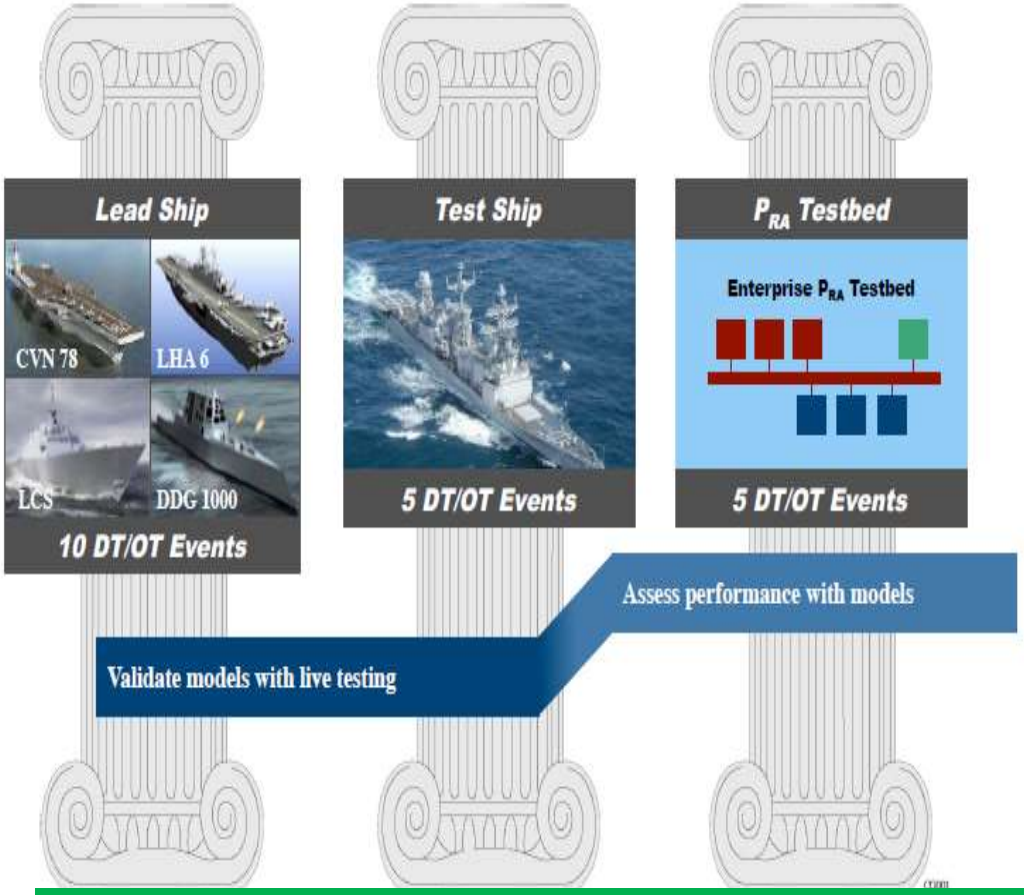
Struck by two Iraqi Exocet Anti Ship Cruise Missiles

Challenges to Measuring P_{RA}

- **The probabilistic nature of the P_{RA} requirement and its numeric value would be too expensive to demonstrate via a traditional live-fire only test**
- **Range safety restrictions would not allow testers to fly ASCM surrogates close enough to manned ships to allow for self-defense engagements**
- **Coordinating the testing of multiple oversight and non-oversight programs, to produce a final P_{RA} assessment for the SoS**
- **Finding a robust solution that can be applied to other ship classes**

To overcome these challenges, the Navy developed a hybrid strategy of live testing and M&S, known as the Ship Self-Defense Enterprise, to satisfy both element and system of system test T&E requirements

P_{RA} Assessment Strategy
(Test Construct Example)



P_{RA} Assessment

The Navy's P_{RA} assessment strategy is documented in the Air Warfare Ship Self Defense Enterprise TEMP and describes system and system of system level test requirements

Ship Self Defense Results

- **End-to-end testing revealed significant differences in combat system performance against single threats and multiple threat raids:**
  - ESSM performance was greatly affected by raid type
  - RAM and ESSM missile-target pairing was degraded
  - SPQ-9B radar performance against certain types of threats was degraded
- **End-to-end testing supported DOT&E Air Warfare Ship Self Defense *Mission Assessments* for LPD 17 and for CVN 68 class ships**
- **The P_{RA} Test Bed was to measure LPD 17's P_{RA} requirement**
  - Building on its success the Navy is using the P_{RA} Test Bed as system engineering tool to evaluate potential combat system upgrades to the LPD 17 class against various anti-ship cruise missiles
- **Subsequent SoS level tests for LHA 6 and CVN 68 lead to multiple Failure Review Boards that prompted the Navy to create the Fire Control Loop Improvement Program**

Without SoS tests, deficiencies would have remained unknown

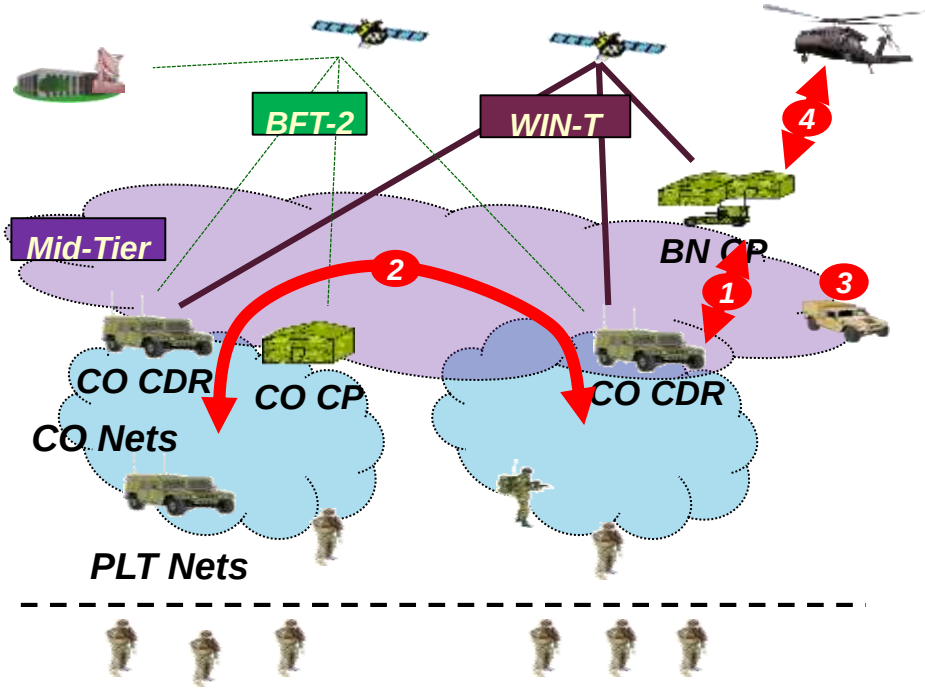
Army Network Integration Evaluation
(Test Construct Example)

- **The Army initiated the Network Integration Evaluation (NIE) in 2011 at Fort Bliss/White Sands Missile Range to test network and communication systems in a system of systems environment.**
- **The NIE utilizes a fully equipped brigade (2nd Brigade, 1st Armor Division) capable of exercising a diverse set of missions.**
- **Equipment is integrated into Tactical Operations Centers, vehicles and dismounted units in representative ways.**
- **Organic threat is provided by a fully functional opposing force with access to electronic warfare and cyber attackers.**
- **The ability to utilize a full brigade over a very wide area (hundreds of square kilometers) allows testers to test multiple systems simultaneously in a representative environment.**

The NIE allows testers to put network and communications systems in a system of systems environment. We can evaluate the performance of system and isolate effects that other systems can have.

Example – Mid-tier Networking Vehicular Radio (MNVR)

- MNVR is a two-channel tactical radio meant to bridge upper- and lower-tactical voice and data networks; it is intended to provide a terrestrial network in satellite denied environments
- MNVR has its own requirements, but must also support the mission command applications that rely on it (primarily the Joint Battle Command-Platform, JBC-P)
- Soldiers must use the Joint Enterprise Network Manager (JENM) to plan, configure, and load the MNVR during combat operations



BFT2 – Blue Force Tracker 2

MNVR SoS Results

- **Soldiers rarely transmitted data traffic over the primary MNVR data network (WNW) during testing contrary to the Army's intended use of WNW**
  - Developmental testing showed the waveform was capable of much more load
- **In satellite-denied environment, message completion rate was significantly degraded**
  - 1st Battalion, 6th Infantry had to dedicate up to 10 percent of combat power for security of MNVR retransmission vehicles, which were necessary to maintain the network
- **The latency of the WNW network was below requirements for the Joint Battle Command-Platform – but MNVR does not have an organic latency requirement.**
- **Soldiers were not able to use the JENM**

Developmental testing showed that MNVR met many of its system specific requirements. SoS testing showed that it doesn't support the applications that run on its waveforms and is not being used as intended

Example – E-3G Airborne Warning and Control System (AWACS) Block 40/45 Upgrade

- **The E-3 AWACS provide airborne early warning, air surveillance, air battle management, and command and control without the beyond line-of-sight limitations inherent in ground-based air battle management systems**

- **The Block 40/45 upgrade replaces the mission computing system on the E-3 with open-architecture, commercial off-the-shelf hardware including servers, and 15 mission crew interactive displays**
  - This upgrade included a re-development of the E-3G's Link-16 integration

E-3G SoS in Large Force Exercises
(Test Construct Example)

- **IOT&E consisted of Block 40/45 E-3 participating in several large force exercises**
  - Included flights working with assets from all four Services in training areas on both coasts as well as over land
- **Post IOT&E data collection during operational inter-agency SoS context provided additional data and insights into system limitations not provided by the IOT&E scope**
- **The fighter, threat, command and control operational envelope of these exercises provided operationally relevant effectiveness and suitability data of the system under test including feedback from operators in the other participating platforms**

The E-3G example is a good illustration of leveraging military exercises to satisfy SoS testing requirements

E-3G SoS Results

- **Tests yielded meaningful findings related to shortcomings in the implementation of Link 16 in the Block 40/45 modified E-3 AWACS**
- **The re-design of Link 16 implementation limited the allocation of time slots to transmit E-3G surveillance tracks to network participants**
- **Flexibility to interleave the Block 40/45 AWACS radar Maritime Surveillance Mode with the Air Surveillance Mode was dropped in the Block 40/45 design**
- **Difficulty in initiating and maintaining maritime surveillance tracks for transmission over Link 11 and Link 16 data links**

SoS Testing Revealed Important Block 40/45 Deficiencies

Example - Battle Control System-Fixed (BCS-F)

- **BCS-F Consolidates radar, flight plan, and other data to provide a near real-time, comprehensive air picture in support of Homeland defense**
  - Integrates input from 200 radars
  - Incorporates tactical data links with interceptor aircraft and C3 assets
  - Includes FAA Flight Plans to aid in threat identification
- **Provides air picture to decision makers at National Military Command Center, AF-North Air Operations Center, and North American Aerospace Defense Command-Northern Command**
- **System Support Facility (SSF) at Tyndall AFB, FL serves as the BCS-F test bed.**
- **BCS-F operates in two CONUS sectors: Tacoma, WA and Rome NY, and in two Regional sectors: Hawaii and Alaska**

BCS-F SoS System Support Facility
(Test Construct Example)

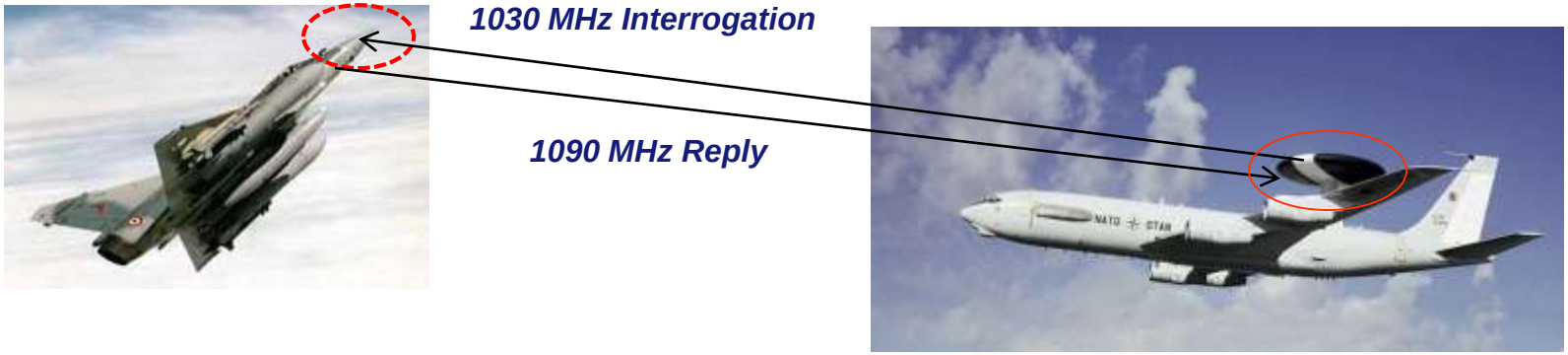
- **Does not replicate the radar feeds and flight plan inputs of the sector facilities**
- **Each sector has a unique architecture for high-side sensor data, routers, switches, cable paths, etc. that is not replicated at SSF**
- **SSF cannot replicate the way each sector utilizes BCS-F functionality to support missions tasks**
- **Real world data links cannot be adequately replicated**
- **SoS testing for BCS-F can only be accomplished live at the CONUS and regional sectors**

BCS-F SoS Results

- **Testing at sector facilities showed that incorporation of Joint Land Attack Cruise Missile Defense Elevated Netted Sensor (JLENS) data, which was not available at the SSF test bed, could cause dual tracks on the BCS-F air picture**
- **Testing at the Hawaii Regional Operations Center revealed deficiencies processing Aircraft Movement Information System (AMIS) data with BCS-F**
  - The Hawaii regional sector is the only sector that uses AMIS data
- **Cyber security testing at regional centers identified cyber vulnerabilities, associated with live radar feeds, that were not found at the SSF**

Example - Mark XIIA Mode 5 Identification Friend or Foe (IFF)

- **Uses classic interrogator / transponder approach to IFF**
  - Adds Mode 5 and Mode S operating modes to existing Mark XII plus a "Lethal Interrogation" capability intended to minimize fratricide
  - Driven by need for secure ID and improved situational awareness
    - New crypto, improved processing, and advanced waveform
  - Mode S mandated by need for compatibility with civil ATC system



- **Mode 5 IFF-equipped systems (regardless of manufacturer) must be fully interoperable and able to exchange accurate ID information across all elements of the Joint C3I system**

Mode 5 IFF Joint Operational Test Approach (JOTA)
(Test Construct Example)

- **Each Service (and Allies) developing and fielding unique Mode 5 IFF boxes in their land, sea, and air platforms and systems**
  - Initial Service test approaches were minimal often using only service unique systems to evaluate IFF capabilities
  - Drove DOD to initiate the Joint Operational Test Approach (JOTA) process for Joint IFF Interoperability testing

- **A JOTA test event involves a mixture of Blue and Red forces consisting of a variety of Joint Service and Allied platforms equipped with IFF systems from a variety of manufacturers**
  - Representative operational flight profiles and tactics are used
  - ID data is disseminated through the C3I system using tactical data link (Link 16)

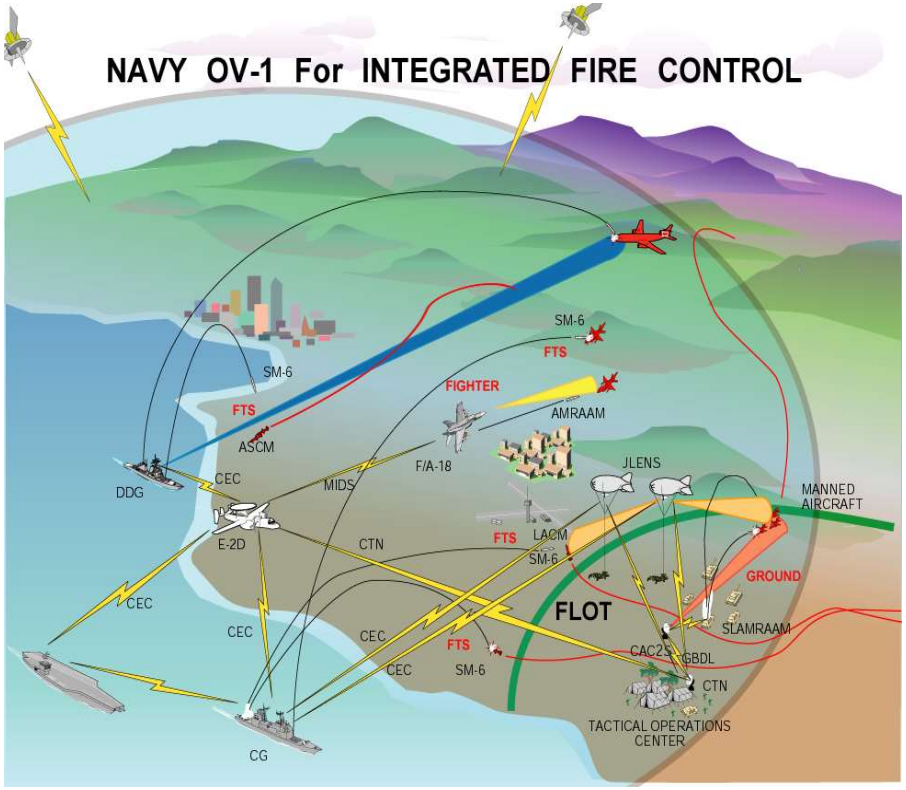
- **Do individual IFF-equipped platforms effectively exchange ID information and facilitate situational awareness across the entire Joint battle arena?**

Mode 5 IFF JOTA Results

- **JOTA event held off U.S. East Coast during Bold Quest Coalition Capability Demonstration and Assessment event**
  - – SoS mixture of blue and red forces included variety of land, air, and naval platforms under Joint C3I control
  - –Air warfare scenarios conducted under Aegis warship, AWACS, or ground controlled intercept control using operational flight profiles
- **Results**
  - – Aegis initially unable to come online due to incorrect procedures for initialization of its Mode 5 interrogator
  - – Improvements needed in Patriot and Aegis ability to employ Lethal Interrogation capability
  - – ID information could not be reliably passed through the C3I system due to inconsistent implementation of MILSTD for dissemination of Mode 5 messages over Link 16

Example – Planned Testing of Aegis Modernization to include NIFC-CA

- **Aegis Modernization is a planned upgrade to the combat systems of the Navy's existing cruisers and current and future DDG 51 class destroyers**
- **Part of that upgrade is incorporating the NIFC-CA capability into to Aegis combat system**
- **Based on existing requirements, NIFC-CA allows Aegis ships to utilize the E-2D Advanced Hawkeye's improved surveillance capability and the long range capability of the SM-6 standard missile**



Aegis / NIFC-CA SoS tests

- **The Navy does not intend to conduct NIFC-CA operational tests because NIFC-CA is not a program of record, but Aegis Modernization operational testing must demonstrate the NIFC-CA capability**
- **For these Aegis/NIFC-CA tests, the necessary SoS consists of an Aegis DDG/CG, SM-6, E-2D and the cooperative engagement capability**
- **Testing is planned for FY20/21**
- **Results: TBD**

The ability of Aegis to employ the NIFC-CA capability can only be demonstrated in an SoS context

Outline

- **Introduction**
- **How do we test a system in a SoS**
- **Test Constructs and Examples**
- **Resolving Risk in 2020**

Resolving Risk in 2020

- **Testing in a SoS environment reveals systems engineering problems that would not otherwise be found**
- **An active IPT is important to make sure that testing is effectively coordinated across each participating acquisition program and to coordinate with legacy programs.**
- **OTA and DOT&E participation is critical to ensure that planned test events support data requirements**
- **Coordinating SoS testing is challenging but it can be made easier via an Enterprise-like solution**
- **For systems not yet developed, make sure that requirements documents include mission success oriented metrics for the entire SoS**