ASN (RDA)
Chief Engineer

System Engineering Re-vitalization within DoN Status

25 October 2005

Mr. Carl Siel
ASN(RDA) Chief Engineer
carl.siel@navy.mil

Unclassified

Reinvigoration of Systems Engineering

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION, TECHNOLOGY AND LOGISTICS

FEB 20 2004

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Policy for Systems Engineering in DoD

Application of rigorous systems engineering discipline is paramount to the Department's ability to meet the challenge of developing and maintaining needed warfighting capability. This is especially true as we strive to integrate increasingly complex systems in a family-of-systems, system-of-systems, net-centric warfare context. Systems engineering provides the integrating technical processes to define and balance system performance, cost, schedule, and risk. It must be embedded in program planning and performed across the entire acquisition life cycle.

Toward that end, I am establishing the following policy, effective immediately and to be included in the next revision of the DoD 5000 series acquisition documents:

Systems Engineering (SE). All programs responding to a capabilities or requirements document, regardless of acquisition category, shall apply a robust SE approach that balances total system performance and total ownership costs within the family-of-systems, systems-of-systems context. Programs shall develop a Systems Engineering Plan (SEP) for Milestone Decision Authority (MDA) approval in conjunction with each Milestone review, and integrated with the Acquisition Strategy. This plan shall describe the program's overall technical approach, including processes, resources, metrics, and applicable performance incentives. It shall also detail the timing, conduct, and success criteria of technical reviews.

In support of the above policy, the Director, Defense Systems shall:

a. Identify the requirement for a SEP in DODI 5000.2, and provide specific content guidance tailorable by the MDA in the Defense Acquisition Guidebook.

b. Assess the adequacy of current Department-level SE related policies, processes, practices, guidance, tools, and education and training and recommend to me necessary changes.

c. Establish a senior-level SE forum with participation from the Military Departments, and appropriate defense agencies, as a means to collaborate and leverage activities within the components and to provide a forum to institutionalize SE discipline across the Department. A goal of this forum will be extending the SE process to address family-of systems, system-of-systems capability-based acquisition.

d. For programs where I am the MDA, review each program's SEP as part of the preparation for Defense Acquisition Board Milestone Reviews (DAB) and other acquisition reviews, provide me with a recommendation on the program's readiness to proceed during the DAB. Together with other members of the OSD staff, lead program support assessments to identify and help resolve issues to ensure program success.

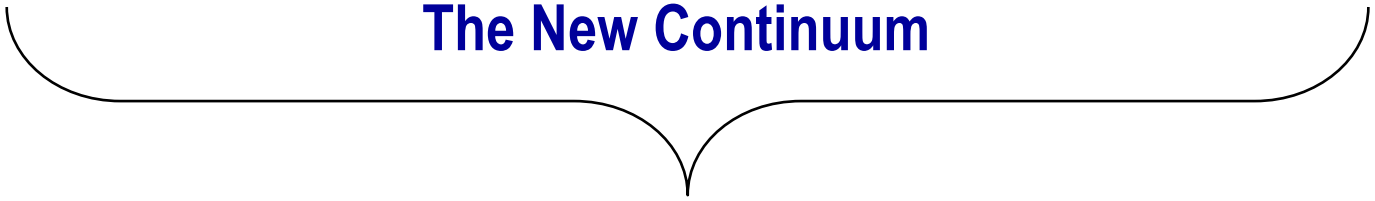
To assist in these efforts, each Component Acquisition Executive and defense agency with acquisition responsibilities will, within 90 days, provide the Director, Defense Systems its approach and recommendations on how we can ensure that application of sound systems engineering discipline is an integral part of overall program planning, management, and execution within both DoD and defense industry. Further, I direct each Component Acquisition Executive and those defense agencies with acquisition responsibilities to provide, within 30 days, a flag officer or Senior Executive Service-level representative to participate in the Director, Defense Systems-led systems engineering forum. The first such forum will be held within 60 days.

I need your assistance to ensure we drive good systems engineering processes and practices back into the way we do business. We can accomplish this goal by establishing clear policies, reinvigorating our training, developing effective tools, and using and *institutionalizing best* practices, applying performance incentives, and making systems engineering an important consideration during source selections and throughout contract execution. Collectively these actions will reinvigorate our acquisition community - including our industry partners - thus assuring affordable, supportable, and above all, *capable solutions for the warfighter.*

Michael W. Wynne
Acting

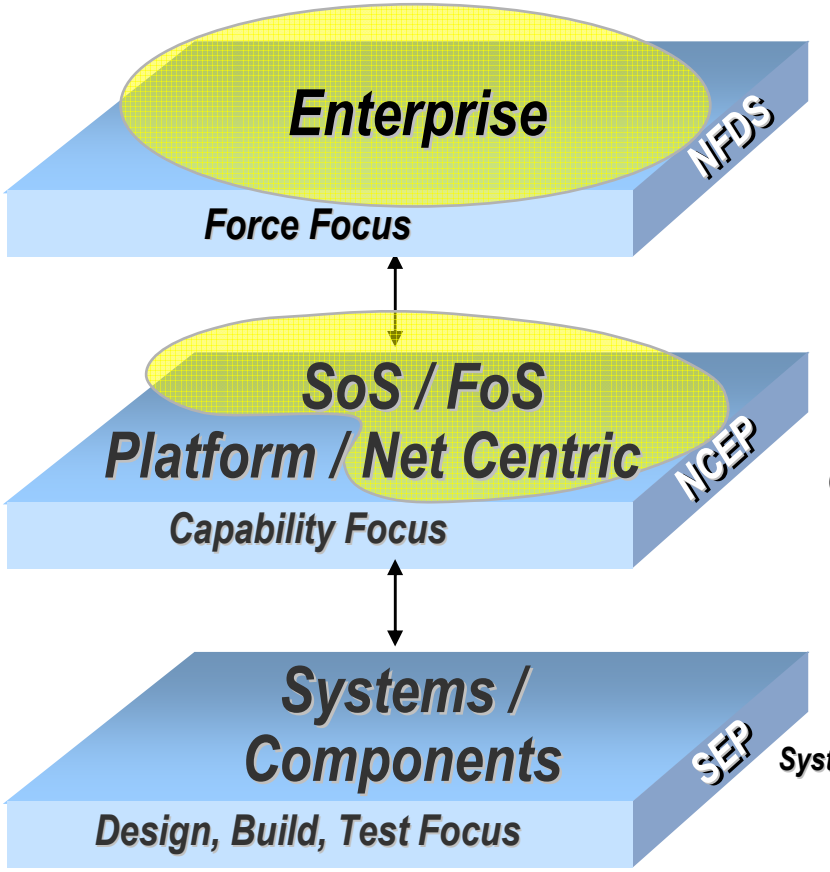
Purpose

- Up-date you on some of our activities since last year
- Use the opportunity to stimulate you on our common challenge: *Capability-Based Systems Engineering*



Enterprise ⟺ FoS/SoS ⟺ Systems

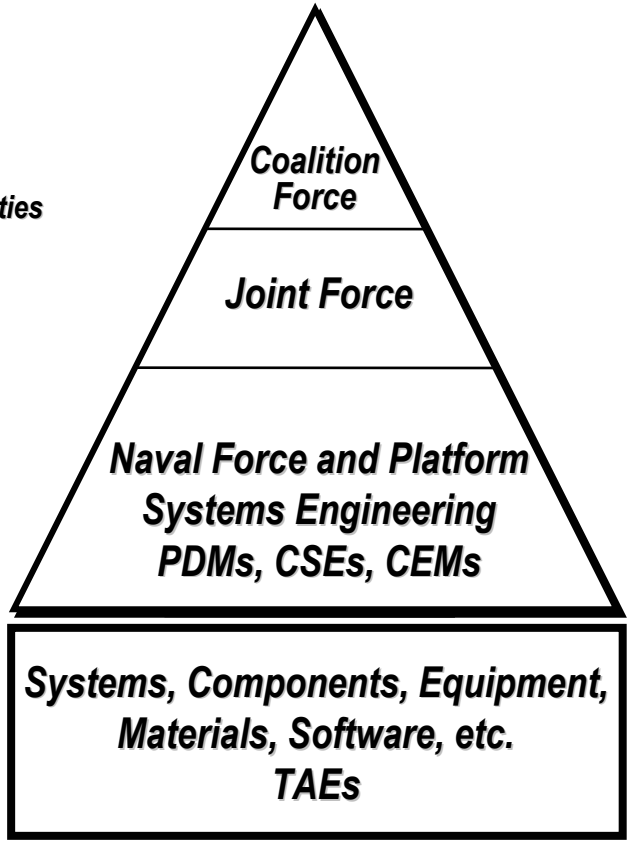
Capability-Based System Engineering



Translates
Operational Concepts → Capabilities

Translates
Capabilities → System Requirements

Translates
System Requirements → End Items



Requires Alignment of Multiple Processes, Process Owners and Products

Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of Systems Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

Scope

Marine Corps
System Command

NAVSEA
NAVAL SEA SYSTEMS COMMAND

Naval Sea
System Command

Naval Air
System Command

SPAWAR

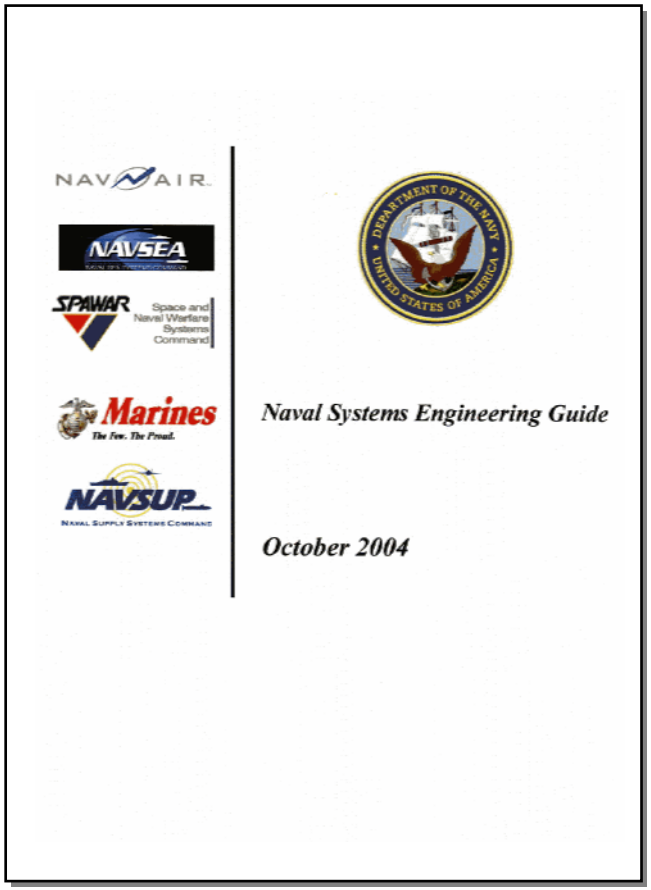
Space: Naval Warfare
Systems Command

Must address the full range of Land, Sea, Undersea, Air and Space applications/operative environments

Topics

- **Virtual System Commands**
  - Naval Systems Engineering Guide
  - Engineering Technical Authority
  - Risk Management Process
  - Systems Engineering Technical Review Process
  - System Certification Policy
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of Systems Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

Naval System Engineering Guide

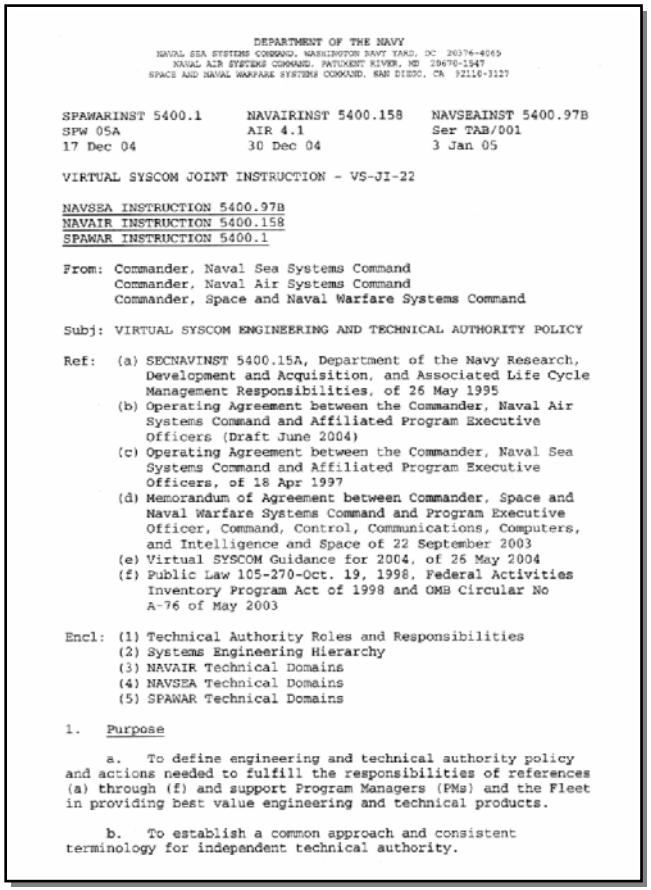


Purpose:

- Characterize the contents of the Systems Engineering Discipline
- Promote a consistent and common view of Systems Engineering across the Navy
- Clarify the boundary of Systems Engineering with respect to other disciplines
- Provide a foundation for curriculum development and Systems Engineering Certification

Status: Completed Oct 04

Engineering and Technical Authority



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND, WASHINGTON NAVY YARD, DC 20376-4065
NAVAL AIR SYSTEMS COMMAND, PATUXENT RIVER, MD 20670-1547
SPACE AND NAVAL WARFARE SYSTEMS COMMAND, SAN DIEGO, CA 92110-3127

SPAWARINST 5400.1	NAVAIRINST 5400.158	NAVSEAINST 5400.97B
SPW 05A	AIR 4.1	Ser TAB/001
17 Dec 04	30 Dec 04	3 Jan 05

VIRTUAL SYSCOM JOINT INSTRUCTION - VS-JI-22

NAVSEA INSTRUCTION 5400.97B
NAVAIR INSTRUCTION 5400.158
SPAWAR INSTRUCTION 5400.1

From: Commander, Naval Sea Systems Command
Commander, Naval Air Systems Command
Commander, Space and Naval Warfare Systems Command

Subj: VIRTUAL SYSCOM ENGINEERING AND TECHNICAL AUTHORITY POLICY

Ref: (a) SECNAVINST 5400.15A, Department of the Navy Research, Development and Acquisition, and Associated Life Cycle Management Responsibilities, of 26 May 1995
(b) Operating Agreement between the Commander, Naval Air Systems Command and Affiliated Program Executive Officers (Draft June 2004)
(c) Operating Agreement between the Commander, Naval Sea Systems Command and Affiliated Program Executive Officers, of 18 Apr 1997
(d) Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command and Program Executive Officer, Command, Control, Communications, Computers, and Intelligence and Space of 22 September 2003
(e) Virtual SYSCOM Guidance for 2004, of 26 May 2004
(f) Public Law 105-270-Oct. 19, 1998, Federal Activities Inventory Program Act of 1998 and OMB Circular No A-76 of May 2003

Encl: (1) Technical Authority Roles and Responsibilities
(2) Systems Engineering Hierarchy
(3) NAVAIR Technical Domains
(4) NAVSEA Technical Domains
(5) SPAWAR Technical Domains

1. Purpose

a. To define engineering and technical authority policy and actions needed to fulfill the responsibilities of references (a) through (f) and support Program Managers (PMs) and the Fleet in providing best value engineering and technical products.

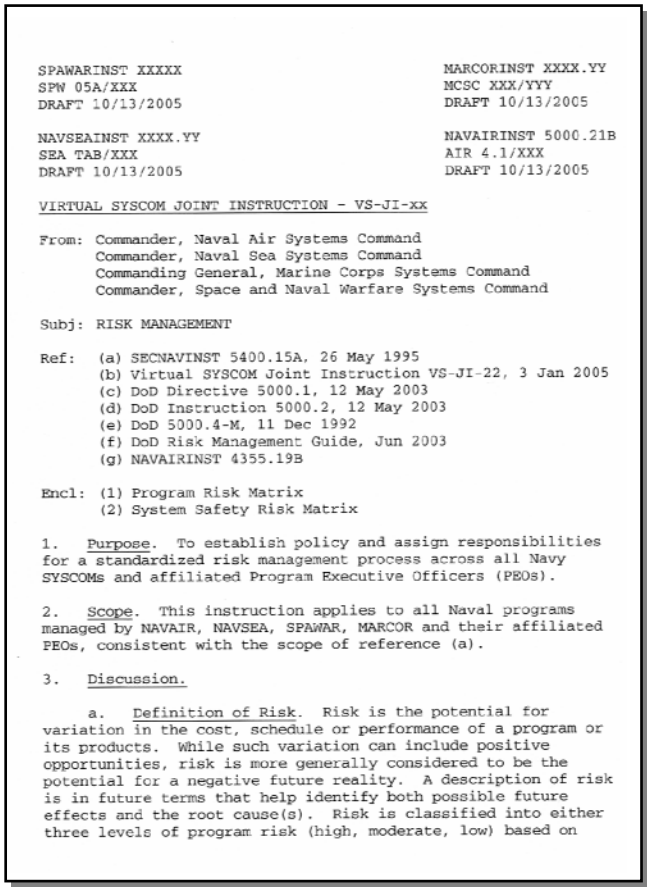
b. To establish a common approach and consistent terminology for independent technical authority.

Purpose:

- Define Engineering and Technical Authority Policy
- Establish a common approach and consistent terminology
- Describle Inter-relationship between Technical Authority and related disciplines (e.g., programmatic and certification authority)

Status: Completed Jan 05

Risk Management Process



SPAWARINST XXXXX
SPW 05A/XXX
DRAFT 10/13/2005

MARCORINST XXXX.YY
MCSC XXX/YYY
DRAFT 10/13/2005

NAVSEAINST XXXX.YY
SEA TAB/XXX
DRAFT 10/13/2005

NAVAIRINST 5000.21B
AIR 4.1/XXX
DRAFT 10/13/2005

VIRTUAL SYSCOM JOINT INSTRUCTION - VS-JI-xx

From: Commander, Naval Air Systems Command
Commander, Naval Sea Systems Command
Commanding General, Marine Corps Systems Command
Commander, Space and Naval Warfare Systems Command

Subj: RISK MANAGEMENT

Ref: (a) SECNAVINST 5400.15A, 26 May 1995
(b) Virtual SYSCOM Joint Instruction VS-JI-22, 3 Jan 2005
(c) DoD Directive 5000.1, 12 May 2003
(d) DoD Instruction 5000.2, 12 May 2003
(e) DoD 5000.4-M, 11 Dec 1992
(f) DoD Risk Management Guide, Jun 2003
(g) NAVAIRINST 4355.19B

Encl: (1) Program Risk Matrix
(2) System Safety Risk Matrix

1. Purpose. To establish policy and assign responsibilities for a standardized risk management process across all Navy SYSCOMs and affiliated Program Executive Officers (PEOs).

2. Scope. This instruction applies to all Naval programs managed by NAVAIR, NAVSEA, SPAWAR, MARCOR and their affiliated PEOs, consistent with the scope of reference (a).

3. Discussion.

a. Definition of Risk. Risk is the potential for variation in the cost, schedule or performance of a program or its products. While such variation can include positive opportunities, risk is more generally considered to be the potential for a negative future reality. A description of risk is in future terms that help identify both possible future effects and the root cause(s). Risk is classified into either three levels of program risk (high, moderate, low) based on

Purpose: Establish Policy and assign responsibilities for standardized risk management process across all Navy SYSCOMs and affiliated Program Executive Officers (PEOs)

Status: Working Draft – Estimated completion date Dec 05

System Engineering Technical Review

Interim Version
1.4B
11/17/04

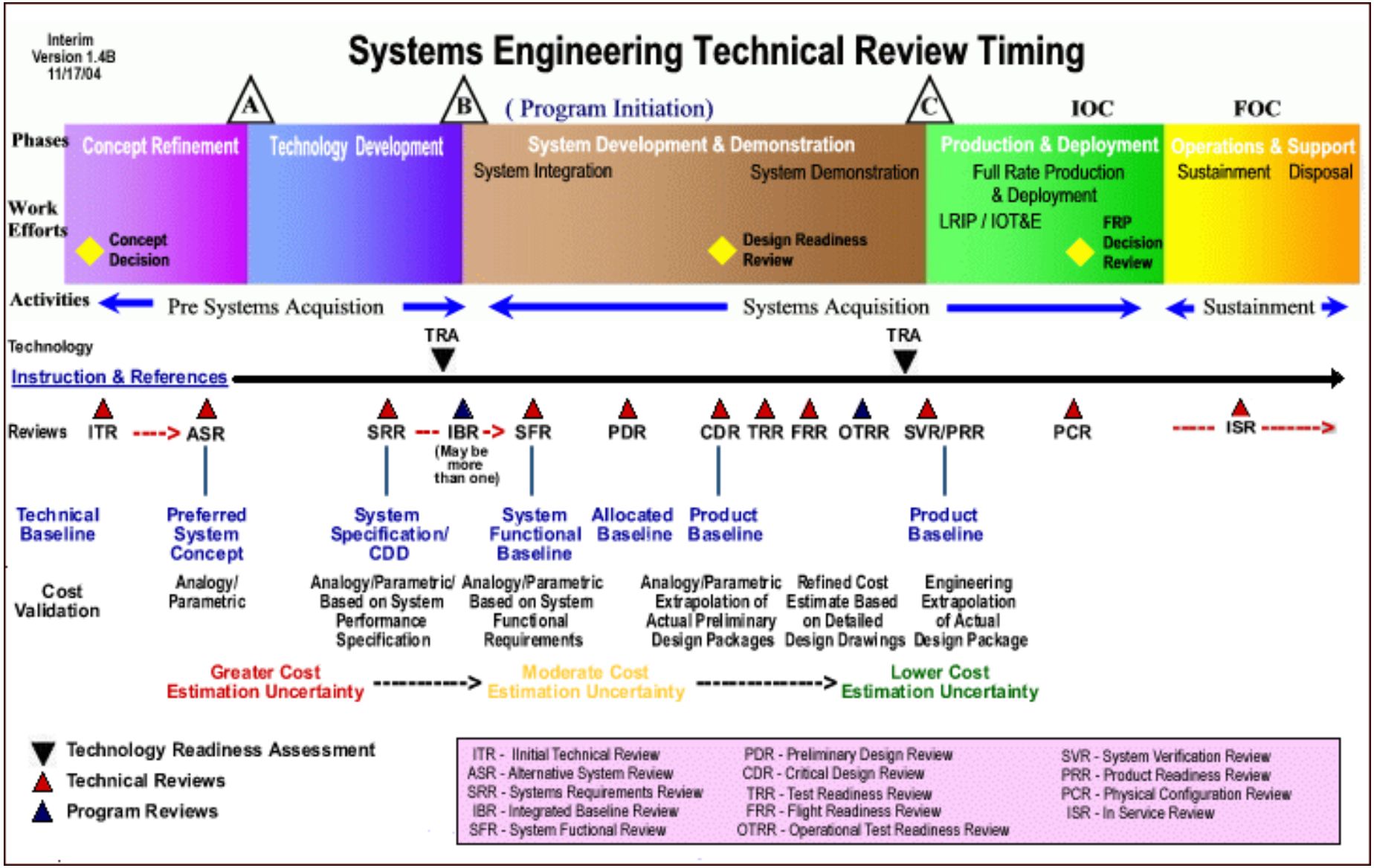
Welcome To The Interactive SETR Timeline

To Begin, Simply Click The Link Below!

Systems Engineering Technical Review Timeline

The SETR Timeline Has ▲ Indicating Each Review. By Placing Your Cursor On These You Can Select It's Corresponding Documentation. There Is Also A Link In Blue Instruction & References For Additional Documents.

https://www.kmsonline.net/41G/KMS/Library/index.htm


Interim
Version 1.4B
11/17/04
Systems Engineering Technical Review Timing
A
B
(Program Initiation)
C
IOC
FOC
Phases
Concept Refinement
Technology Development
System Development & Demonstration
System Integration
System Demonstration
Production & Deployment
Full Rate Production & Deployment
LRIP / IOT&E
Operations & Support
Sustainment
Disposal
Work Efforts
Concept Decision
Design Readiness Review
FRP Decision Review
Activities
Pre Systems Acquistion
Systems Acquisition
Sustainment
Technology
TRA
TRA
Instruction & References
Reviews
ITR
ASR
SRR
IBR
(May be more than one)
SFR
PDR
CDR
TRR
FRR
OTRR
SVR/PRR
PCR
ISR
Technical Baseline
Preferred System Concept
System Specification/ CDD
System Functional Baseline
Allocated Baseline
Product Baseline
Product Baseline
Cost Validation
Analogy/ Parametric
Analogy/Parametric/ Based on System Performance Specification
Analogy/Parametric Based on System Functional Requirements
Analogy/Parametric Extrapolation of Actual Preliminary Design Packages
Refined Cost Estimate Based on Detailed Design Drawings
Engineering Extrapolation of Actual Design Package
Greater Cost Estimation Uncertainty
Moderate Cost Estimation Uncertainty
Lower Cost Estimation Uncertainty
Technology Readiness Assessment
Technical Reviews
Program Reviews
ITR - Iinitial Technical Review
ASR - Alternative System Review
SRR - Systems Requirements Review
IBR - Integrated Baseline Review
SFR - System Fuctional Review
PDR - Preliminary Design Review
CDR - Critical Design Review
TRR - Test Readiness Review
FRR - Flight Readiness Review
OTRR - Operational Test Readiness Review
SVR - System Verification Review
PRR - Product Readiness Review
PCR - Physical Configuration Review
ISR - In Service Review

Preliminary Design Review

PDR – Preliminary Design Review

1. Purpose - The Preliminary Design Review (PDR) is a multi-disciplined product and process assessment to ensure that the system under review can proceed into detailed design, and can meet the stated performance requirements within cost (program budget), schedule (program schedule), risk, and other system constraints. Generally this review assesses the system preliminary design as captured in performance specifications for each configuration item in the system (allocated baseline), and ensures that each function in the functional baseline has been allocated to one or more system configuration items. Configuration items may consist of hardware and software elements, and include items such as airframe, avionics, weapons, crew systems, engines, trainers/training, etc.

For complex systems, a PDR may be conducted for each subsystem or configuration item. These incremental reviews would lead up to an overall system PDR. When incremental reviews have been conducted, the emphasis of the overall system PDR should be on configuration item functional and physical interface design, as well as overall system design requirements. PDR determines whether the hardware, human and software preliminary designs are complete, and the IPT is prepared to start detailed design and test procedure development.

The subsystem requirements are evaluated to determine whether they correctly and completely implement all system requirements allocated to the subsystem, and whether traceability of subsystem requirements to system design is maintained. At this review the IPT should also review the results of peer reviews on requirements and preliminary design documentation. A successful review is predicated on the IPT's determination that the subsystem requirements, subsystem preliminary design, results of peer reviews, and plans for development and testing form a satisfactory basis for proceeding into detailed design and test procedure development.

The review may be tailored in accordance with the technical scope and risk of the system. Under no circumstances should the review be tailored completely out of the development plan. Details of any tailoring should be described in the SEP, or should occur as part of the APMSE or systems engineer coordination of the review elements with the AIR-4.1 cognizant authority (APEO(RDT&E)). Notwithstanding successful completion of the PDR, the contractor remains responsible for the system design/performance requirements within the terms of the contract.

Completion of this review should provide:

a. An established system allocated baseline,
b. An updated risk assessment for SDD,
c. An updated Cost Analysis Requirements Description (CARD) based on the system allocated baseline, and
d. An updated program schedule including system and software critical path drivers
e. An approved Acquisition Logistics Support Plan (ALSP) with updates applicable to this phase

NAVAIR

Preliminary Design Review
Program Risk Assessment Checklist (1 August 2004 version)

For The _____Program
Date:

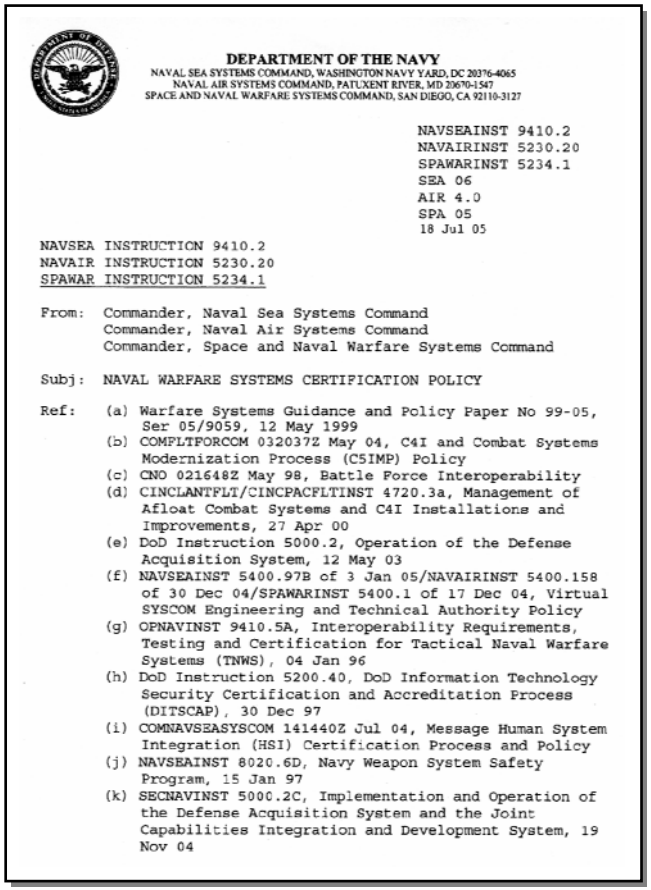
Legend: R Y G U NA

Instructions: Type the appropriate risk character in the space to the right of each question. The risk characters {R,Y,G,U or NA} are not case sensitive. The total number of each character will be displayed in the summary status at the beginning of each section.

R = Red
Y = Yellow
G = Green
U = Unknown/Unavailable
NA = Not Applicable

	R	Y	G	U	NA	Item	Comments/Mitigation
1. Timing / Entry Criteria	0	0	0	0	0	1	
2. Planning	0	0	0	0	0	2	
3. Program schedule	0	0	0	0	0	3	
4. Management metrics relevant to life cycle phase	0	0	0	0	0	4	
5. Program Staffing	0	0	0	0	0	5	
6. Process Review	0	0	0	0	0	6	
7. Requirements Management	0	0	0	0	0	7	
8. FORCEnet Compliance Checklist	0	0	0	0	0	8	
9. Battlespace engineering. Does the preliminary design conform with requirements per JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS) CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION CJCSI 3170.01D 12 March 2004?						9	
10. System Preliminary Design	0	0	0	0	0	10	
11. Program Risk Assessment	0	0	0	0	0	11	
12. Completion/Exit Criteria	0	0	0	0	0	12	

Systems Certification Policy



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND, WASHINGTON NAVY YARD, DC 20376-4065
NAVAL AIR SYSTEMS COMMAND, PATUXENT RIVER, MD 20670-1547
SPACE AND NAVAL WARFARE SYSTEMS COMMAND, SAN DIEGO, CA 92110-3127

NAVSEAINST 9410.2
NAVAIRINST 5230.20
SPAWARINST 5234.1
SEA 06
AIR 4.0
SPA 05
18 Jul 05

NAVSEA INSTRUCTION 9410.2
NAVAIR INSTRUCTION 5230.20
SPAWAR INSTRUCTION 5234.1

From: Commander, Naval Sea Systems Command
Commander, Naval Air Systems Command
Commander, Space and Naval Warfare Systems Command

Subj: NAVAL WARFARE SYSTEMS CERTIFICATION POLICY

Ref: (a) Warfare Systems Guidance and Policy Paper No 99-05, Ser 05/9059, 12 May 1999
(b) COMFLTFORCOM 032037Z May 04, C4I and Combat Systems Modernization Process (C5IMP) Policy
(c) CNO 021648Z May 98, Battle Force Interoperability
(d) CINCLANTFLT/CINCPACFLTINST 4720.3a, Management of Afloat Combat Systems and C4I Installations and Improvements, 27 Apr 00
(e) DoD Instruction 5000.2, Operation of the Defense Acquisition System, 12 May 03
(f) NAVSEAINST 5400.97B of 3 Jan 05/NAVAIRINST 5400.158 of 30 Dec 04/SPAWARINST 5400.1 of 17 Dec 04, Virtual SYSCOM Engineering and Technical Authority Policy
(g) OPNAVINST 9410.5A, Interoperability Requirements, Testing and Certification for Tactical Naval Warfare Systems (TNWS), 04 Jan 96
(h) DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97
(i) COMNAVSEASYSCOM 141440Z Jul 04, Message Human System Integration (HSI) Certification Process and Policy
(j) NAVSEAINST 8020.6D, Navy Weapon System Safety Program, 15 Jan 97
(k) SECNAVINST 5000.2C, Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System, 19 Nov 04

Purpose: Promulgate platform level and strike force level Naval Warfare Systems Certification Policy

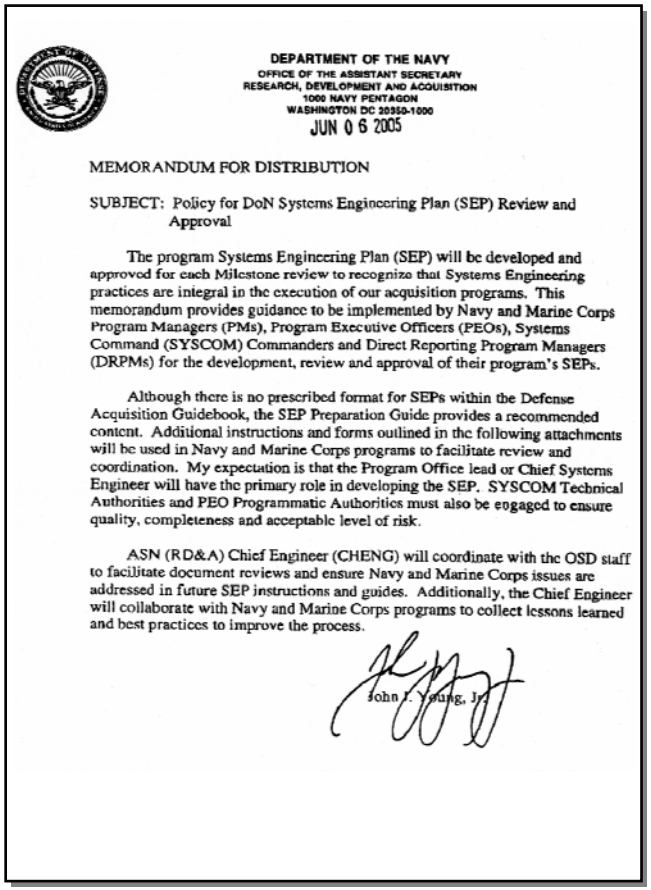
Status:

- Phase I implements Fleet Response Plan (FRP) Compliant Platform Level Certification Policy for Navy surface platforms and introduces Strike Force Certification Policy for all surface platforms- Issued Jul 05
- Phase 2 completes FRP Compliant Platform across SYSCOMs for all platforms and for Strike Force Certification Policy - FY06
- Phase 3 aligns Certification Policy and process with Navy Acquisition Policy – FY07

Topics

- Virtual System Commands
- **ASN (RDA) Policy for Systems Engineering Plan**
- Software Acquisition: Best Practices
- System / System of Systems Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

Policy for DoN Systems Engineering Plan



DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

JUN 06 2005

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Policy for DoN Systems Engineering Plan (SEP) Review and Approval

The program Systems Engineering Plan (SEP) will be developed and approved for each Milestone review to recognize that Systems Engineering practices are integral in the execution of our acquisition programs. This memorandum provides guidance to be implemented by Navy and Marine Corps Program Managers (PMs), Program Executive Officers (PEOs), Systems Command (SYSCOM) Commanders and Direct Reporting Program Managers (DRPMs) for the development, review and approval of their program's SEPs.

Although there is no prescribed format for SEPs within the Defense Acquisition Guidebook, the SEP Preparation Guide provides a recommended content. Additional instructions and forms outlined in the following attachments will be used in Navy and Marine Corps programs to facilitate review and coordination. My expectation is that the Program Office lead or Chief Systems Engineer will have the primary role in developing the SEP. SYSCOM Technical Authorities and PEO Programmatic Authorities must also be engaged to ensure quality, completeness and acceptable level of risk.

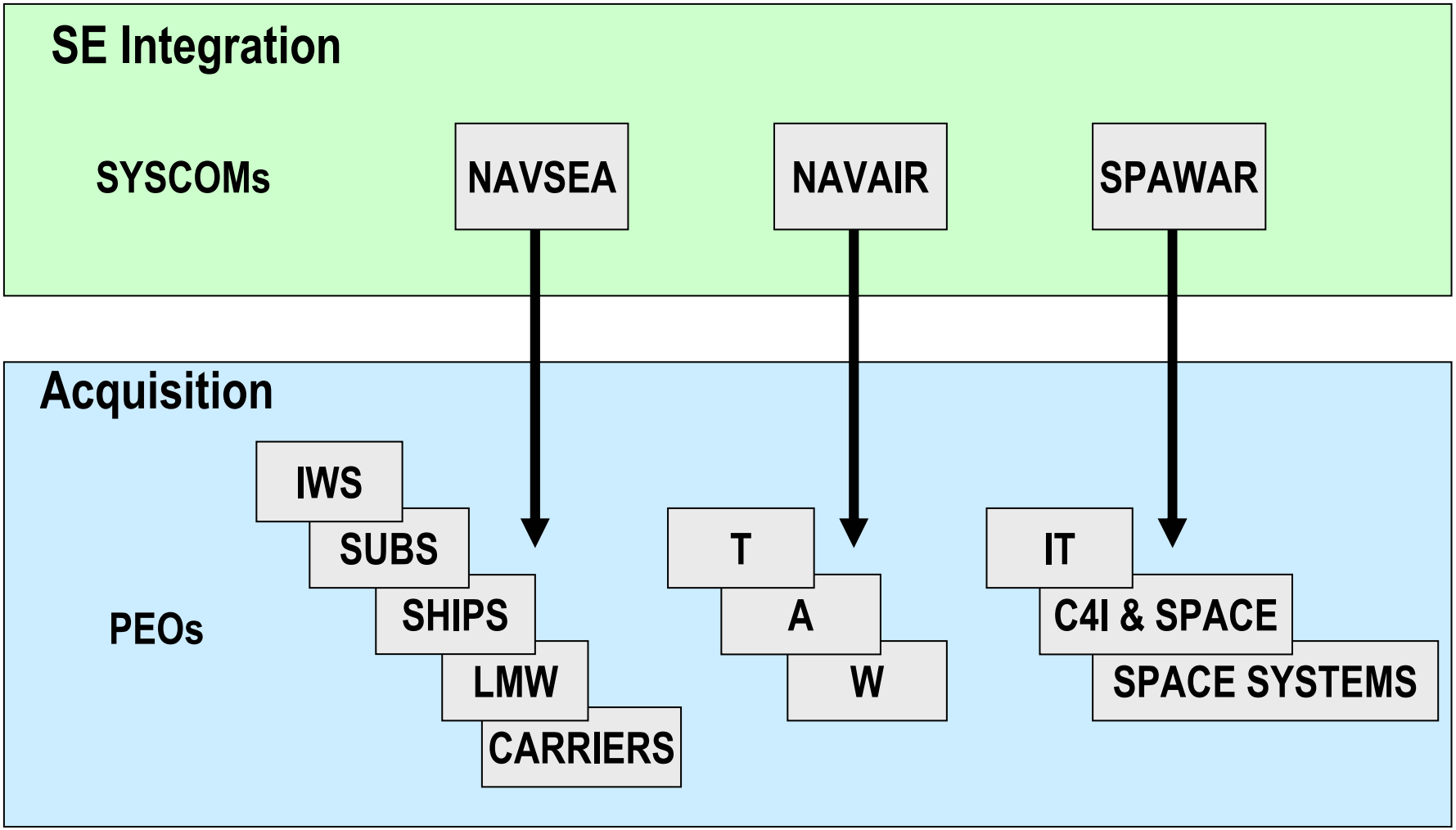
ASN (RD&A) Chief Engineer (CHENG) will coordinate with the OSD staff to facilitate document reviews and ensure Navy and Marine Corps issues are addressed in future SEP instructions and guides. Additionally, the Chief Engineer will collaborate with Navy and Marine Corps programs to collect lessons learned and best practices to improve the process.

John J. Young, Jr.

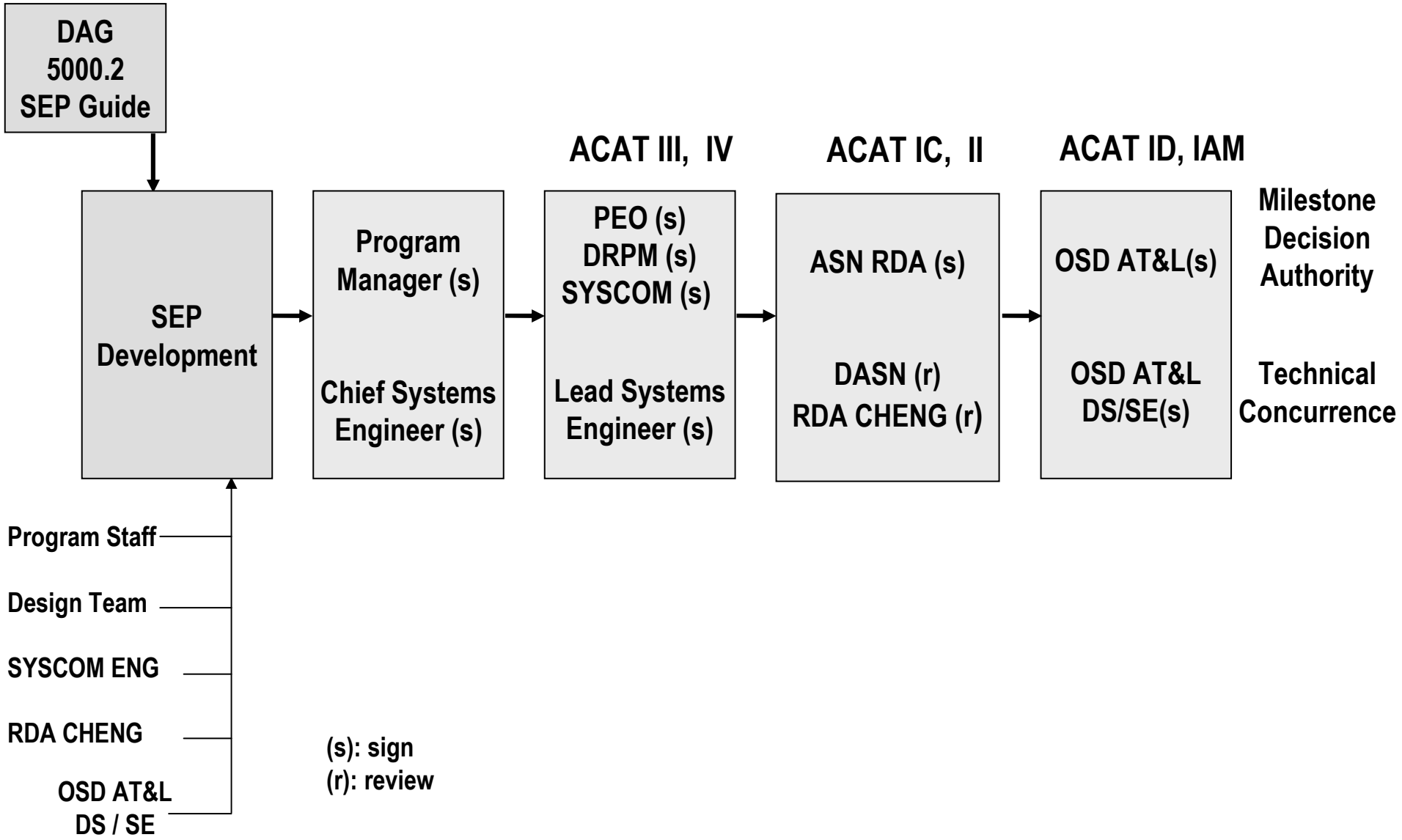
Purpose: Provide guidance for the Development, Review and Approval of Systems Engineering Plans

Status: Promulgated 6 June 05

Navy SE Structure



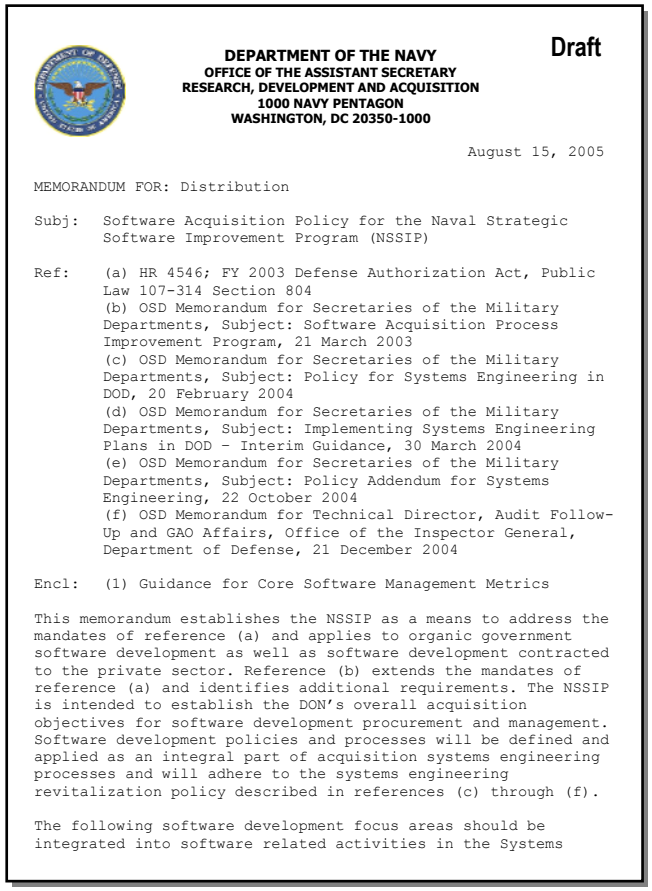
SEP Approval Process



Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- **Software Acquisition: Best Practices**
  - **Software Acquisition Policy**
  - **Software Assurance**
  - **CMMI for Acquisition**
- System / System of Systems Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

Software Acquisition Policy



DEPARTMENT OF THE NAVY
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

Draft

August 15, 2005

MEMORANDUM FOR: Distribution

Subj: Software Acquisition Policy for the Naval Strategic Software Improvement Program (NSSIP)

Ref: (a) HR 4546; FY 2003 Defense Authorization Act, Public Law 107-314 Section 804
(b) OSD Memorandum for Secretaries of the Military Departments, Subject: Software Acquisition Process Improvement Program, 21 March 2003
(c) OSD Memorandum for Secretaries of the Military Departments, Subject: Policy for Systems Engineering in DOD, 20 February 2004
(d) OSD Memorandum for Secretaries of the Military Departments, Subject: Implementing Systems Engineering Plans in DOD – Interim Guidance, 30 March 2004
(e) OSD Memorandum for Secretaries of the Military Departments, Subject: Policy Addendum for Systems Engineering, 22 October 2004
(f) OSD Memorandum for Technical Director, Audit Follow-Up and GAO Affairs, Office of the Inspector General, Department of Defense, 21 December 2004

Encl: (1) Guidance for Core Software Management Metrics

This memorandum establishes the NSSIP as a means to address the mandates of reference (a) and applies to organic government software development as well as software development contracted to the private sector. Reference (b) extends the mandates of reference (a) and identifies additional requirements. The NSSIP is intended to establish the DON's overall acquisition objectives for software development procurement and management. Software development policies and processes will be defined and applied as an integral part of acquisition systems engineering processes and will adhere to the systems engineering revitalization policy described in references (c) through (f).

The following software development focus areas should be integrated into software related activities in the Systems

Purpose

- Establish the Naval Strategic Software Improvement Program as a means to address mandates of Public Law 107-314 Section 804
- Establish DoN's overall acquisition objectives for Software Development, Procurement and Management

Status: Draft-estimated completion date Dec 05

Software Assurance (SwA)

- OSD NII/AT&L Tiger Team established Dec 04 to establish "holistic strategy" and implementation plan
  - Examining potential security issues with (Software) SW
    - Malicious Code insertion
    - Vulnerable Code inadvertently left in COTS/NDI products
- Focus Areas:
  - Engineering-in-Depth (RDA CHENG co-chairs)
  - Prioritization (ID critical systems)
  - Supplier Assurance
  - Science & Technology (tools and mitigation services)
- SwA requirements will be addressed in the SEP and TEMP
  - Leverage existing policy (eg.IA, JCIDS,PPP,etc)

CMMI for Acquisition; CMMI A

- CMMI best practices model for the acquirer being developed – CMMI A
  - Past CMMI models have been for the developer
  - CMMI – Acquisition Module (AM) first attempt at organizing a tool for the acquirer; not successful
- Requirements gathering workshop for the CMMI A to be held on 9 November 2005
  - The plan is to incorporate this model as a "constellation" in version 1.2 of the CMMI model framework

Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- **System / System of Systems Safety**
  - Principal for Safety Certification
  - Systems Safety in Capability-Based Acquisition
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

Principal for Safety Certification

NAVSEAINST 12410.5

Ser

NAVSEA INSTRUCTION 12410.5

From: Commanding Officer, Naval Ordnance Safety and Security Activity

Subj: CERTIFICATION FOR NAVY ACQUISITION PROGRAM PRINCIPAL FOR SAFETY (PFS)

Ref: (a) DODINST 5000.1
(b) DODINST 5000.2
(c) OPNAVINST 5100.24A
(d) DOD 5000.52
(e) DOD 5000.52M
(f) SECNAVINST 12410.22A
(g) MIL-STD-882D

Encl: (1) Definition of Basic Terms
(2) Minimum Requirements for PFS Certification
(3) PFS Certification Program Application Checklist

1. Purpose. To establish policy and guidance for Naval Sea Systems Command (NAVSEA) Principal for Safety (PFS) certification.

2. Scope. This instruction applies to all NAVSEA acquisition programs. Reference (a) requires that a fully proficient acquisition technology and logistics workforce be maintained. It further mandates that system safety engineering and management controls be appropriately applied in the acquisition and life cycle support of DoD weapon systems.

Reference (b) requires that a Program Manager prevent Environment, Safety and Occupational Health (ESOH) hazards where possible, and manage them where they cannot be avoided. Reference (c) requires a trained, and appropriately certified, system safety manager be assigned to each program or system. This manager is to act as the point of contact, for the Program Manager (PM), for system safety matters. References (d), (e), and (f) require the professional development of acquisition workforce personnel, and that assignment of system safety responsibilities only be delegated to qualified personnel.

Point of contact. The NAVSEA point of contact for assistance is The Certification and Standard's Officer, Naval Ordnance Safety and Security Activity, Code XXXXX.

Purpose: Establish policy and guidance for Naval Sea Systems Command Principal for Safety (PFS) Certification

Status: Draft – estimated completion FY06

The U.S. Navy and BCSP Cooperative Agreement

NEWS RELEASE

Contacts:

For Immediate Release:

Jim Gerber

Weapon Syste
(301) 744-601

Heather Murphy, *Communication & Marketing Manager*

Board of Certified Safety Professionals
217/359-9263; heather@bcsp.org

The U.S. Navy and BCSP Establish Cooperative Agreement

Indian Head, Maryland—July 26, 2004—On March 16, 2004, the U.S. Navy's Weapon System Explosives Safety Review Board (WSESRB) and the Board of Certified Safety Professionals (BCSP) established a cooperative agreement for the certification of Navy weapon system safety personnel as Principals for Safety (PFS). WSESRB has established an implementation date of December 31, 2004 for the PFS certification program.

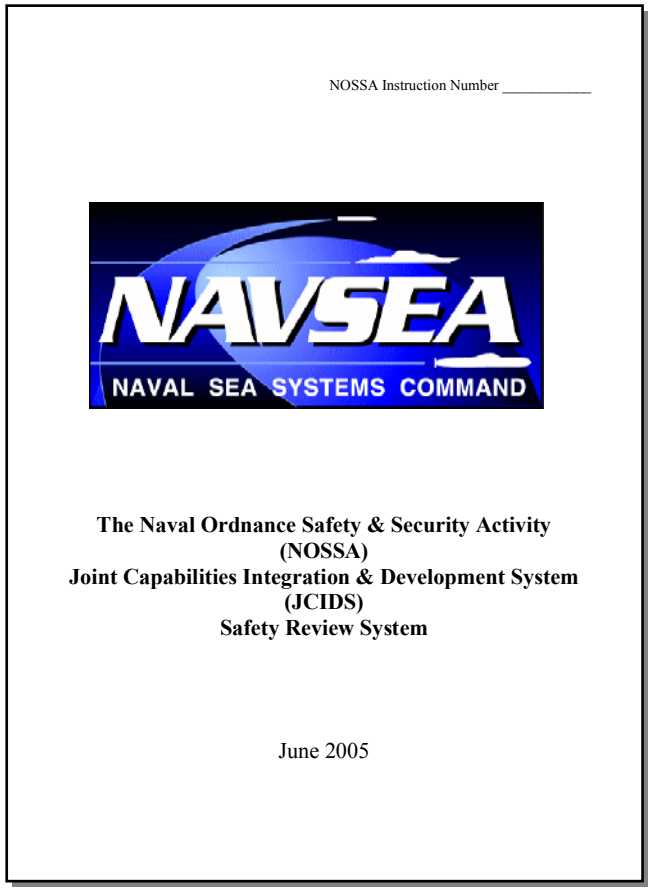
BCSP supports the PFS certification program by managing and operating the examination that PFS candidates must successfully complete to demonstrate competence in system safety concepts. After successfully completing this examination, PFS candidates must finish additional training in weapon system safety concepts and demonstrate competence on another WSESRB-managed examination to earn the PFS certification. WSESRB and BCSP have agreed to maintain the system safety examination in accordance with national and international examination-related accreditation standards.

"BCSP is privileged to cooperate with a leading military safety-centered organization like the WSESRB," said BCSP Executive Director, Roger Brauer, Ph.D., CSP, P.E. "The WSESRB Principal for Safety certification program is a well-designed program that will promote safety professionalism and encourage a continued high level of system safety competence within the WSESRB and the Navy's weapon system safety community."

"By working with BCSP and implementing this high-profile internal safety certification program, the WSESRB can seek to better protect the Navy's personnel and platforms from the risks associated with complex weapon systems in the Fleet," said Edward Kratovil, Chairman of the WSESRB.

…the U.S. Navy's Weapon System Explosives Safety Review Board (WSESRB) and the Board of Certified Safety Professionals (BCSP) established a cooperative agreement for the certification of Navy weapon system safety personnel as Principals for Safety (PFS).

Systems Safety in Capability-Based Acquisition



NOSSA Instruction Number _____

NAVSEA

NAVAL SEA SYSTEMS COMMAND

The Naval Ordnance Safety & Security Activity (NOSSA)
Joint Capabilities Integration & Development System (JCIDS)
Safety Review System

June 2005

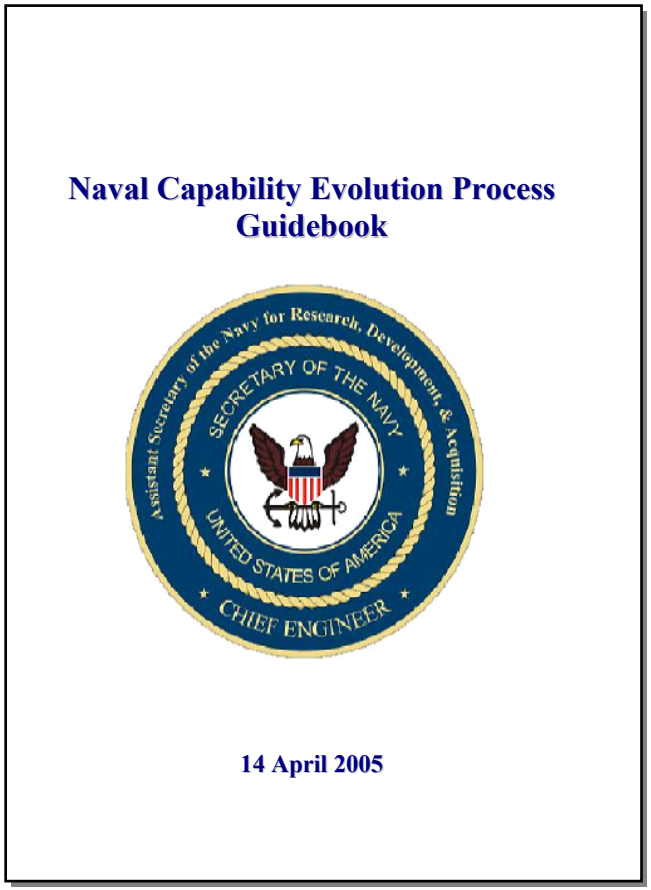
Purpose: Describe a new Naval Ordnance Safety and Security Activity (NOSSA) System for conducting acquisition document safety reviews and for complying with the Joint Capabilities Integration and Development System

Status: Issued Jun 05

Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of System Safety
- **Naval Capability Evolution Process**
  - **Vol I - Guidebook**
  - **Vol II – Best Practices**
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

NCEP Vol I - Guidebook



Purpose:

- Describes The Naval Capability Development Process
- Provides guidance for its use by the DoN acquisition community

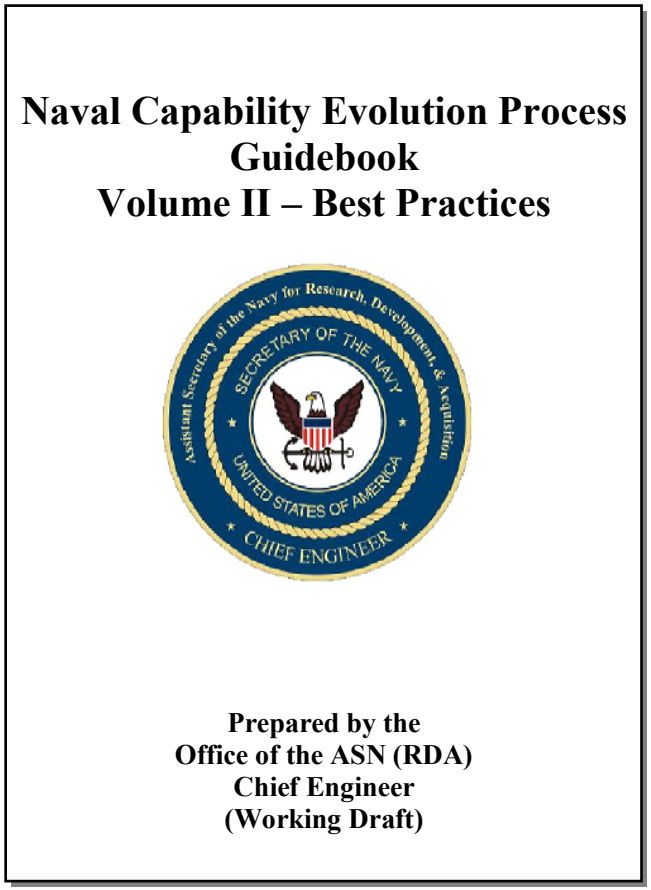
Status: Version 1.1 issued 14 April 05

https://www.asnrdacheng.navy.mil/cheng/general/docs/CHENG.NCEP.v1.Final.pdf

NCEP Vol I - Guidebook

- Aligned with CJCSI-3170.1C, DODI-5000.2, SECNAV-5000.2C
- Key Elements
  - Capability Evolution Planning
    - Current Architecture Assessment (Capability Needs Identification)
    - Capability Alternatives Identification
    - Analysis of Alternatives
    - Capability Evolution Plan
  - Capability Engineering (Abstracted the Systems Engineering Process)
    - Operational Analysis
    - Functional Analysis & Allocation
    - Portfolio Synthesis
    - Portfolio Analysis
  - Portfolio Execution
    - Portfolio Assessment
    - Program Alignment
    - Program Status & Milestone Reviews
  - SE IPT Collaborative Engineering Environment

NCEP Vol II – Best Practices



Purpose:

- Provide recommended methods, techniques and tools that enable execution of activities described by Vol I
- Provide examples of real world problems and uses cases

Status: Draft Version 1.1- estimated completion date Nov 05

https://www.asnrdacheng.navy.mil/cheng/general/docs/CHENG.NCEP.v1.Final.pdf

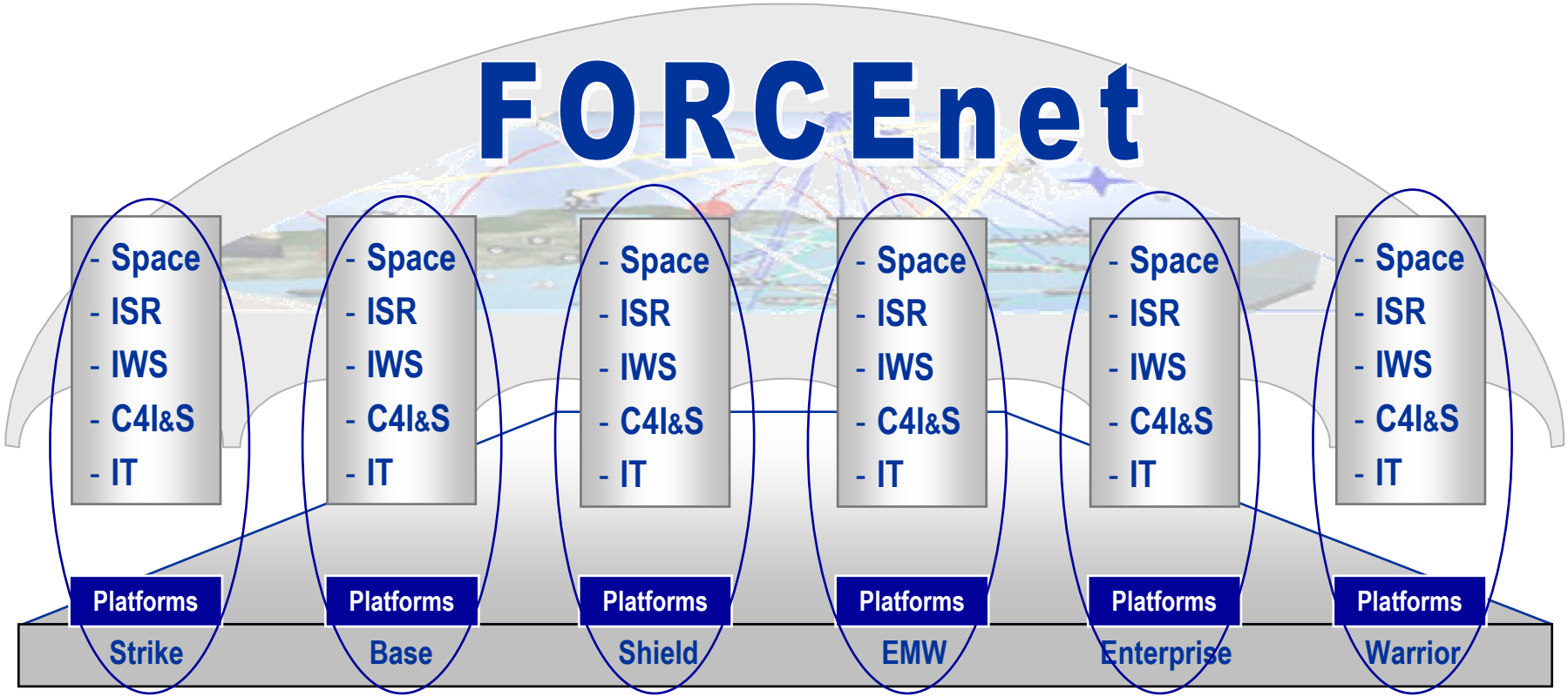
NCEP Vol II – Best Practices

- Capability Specification and Metrics
- Applying QFD to Capability-based Planning
- Role of Architecture
- Capability Evolution Plan
  - Mission Threads/Concept of Operations
  - Capability Evolution Objectives
  - Force Package Structure
  - Readiness Concepts
  - Sustainment Concepts
  - System Service-life Profile
  - Technology Adoption Milestones
  - Force Training and Transition Plan
  - Capability Investment Strategy
  - Acquisition Portfolio Risk Abatement Plan
- Force Package Engineering Models

Topics

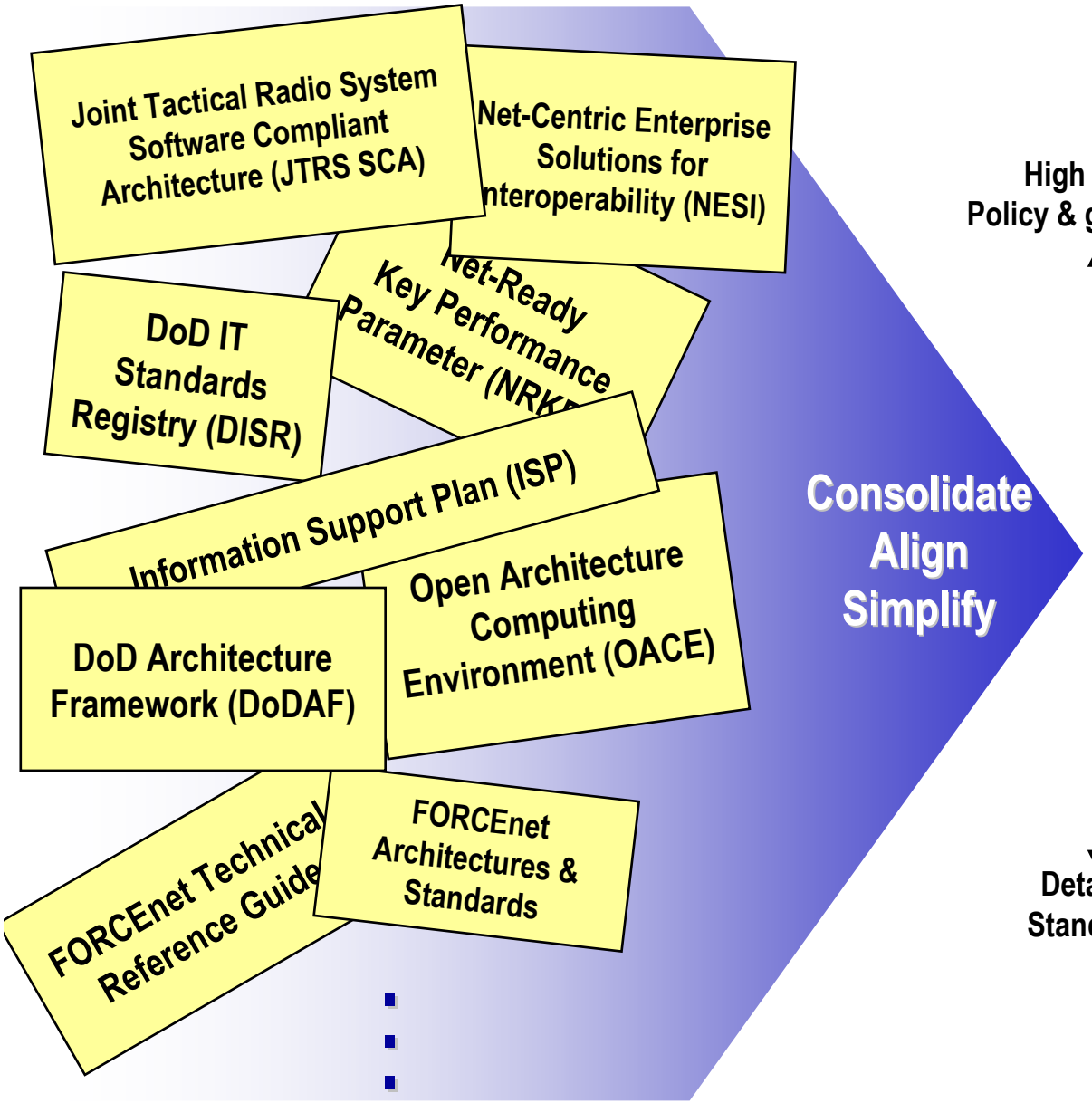
- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of System Safety
- Naval Capability Evolution Process
- **FORCEnet / Open Architecture Integration and Interoperability**
  - **Technical document consolidation**
  - **Test & Evaluation Risk Management**
  - **FORCEnet Integration & Interoperability Management Plan**
- The Technical Cooperation Panel – Technical Panel 4
- Naval Force Development System

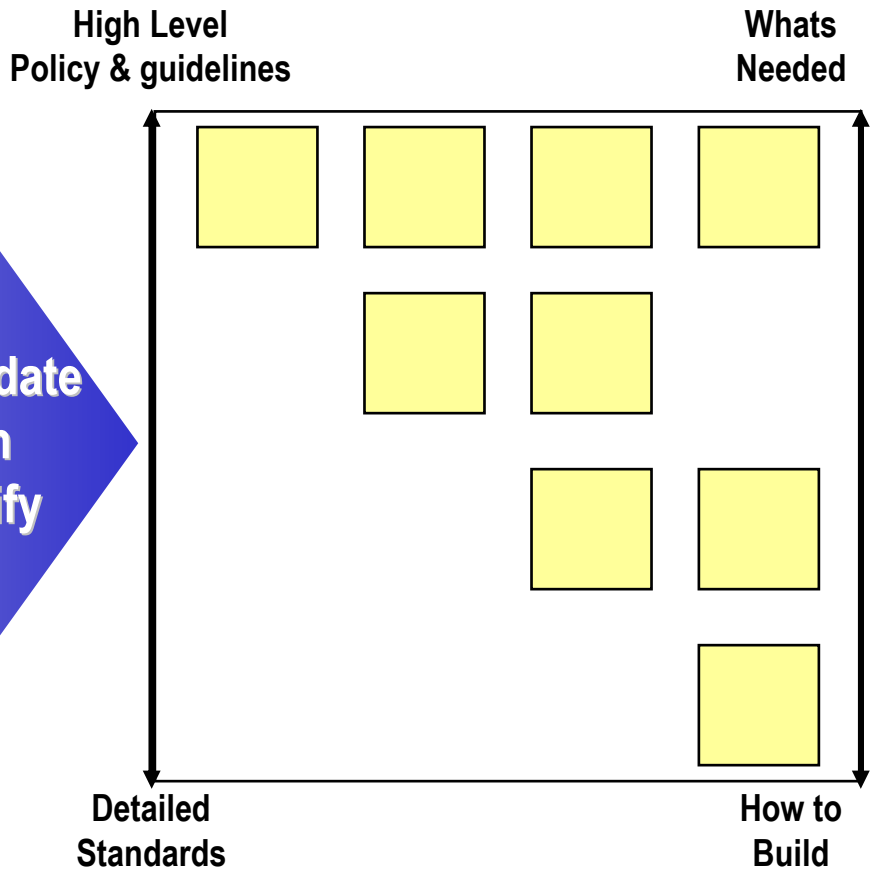
Breadth of FORCEnet



Warfighting + Warfighting Support + Business Systems

Technical Documentation Consolidation

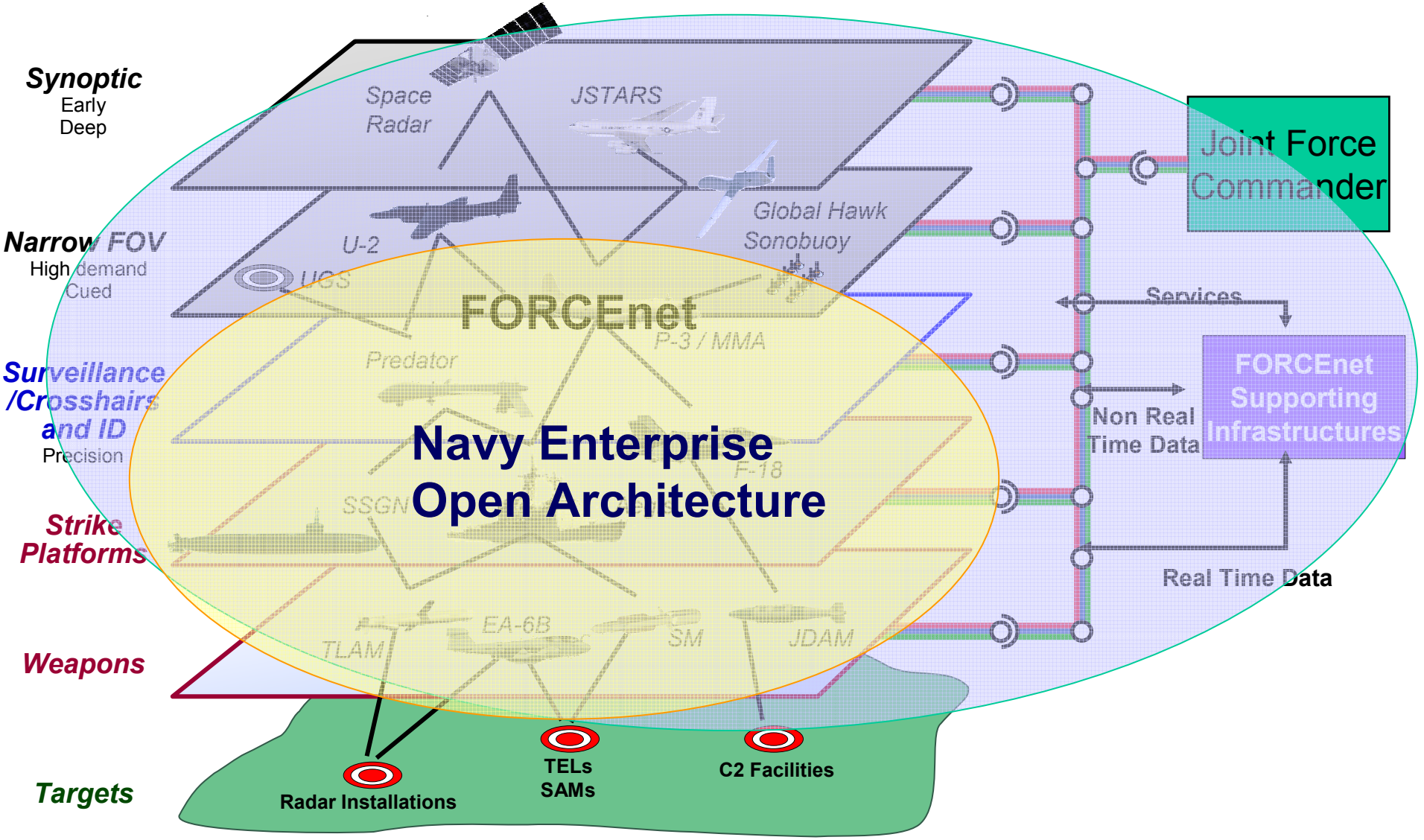




OA/FN Alignment Experimentation Strategy

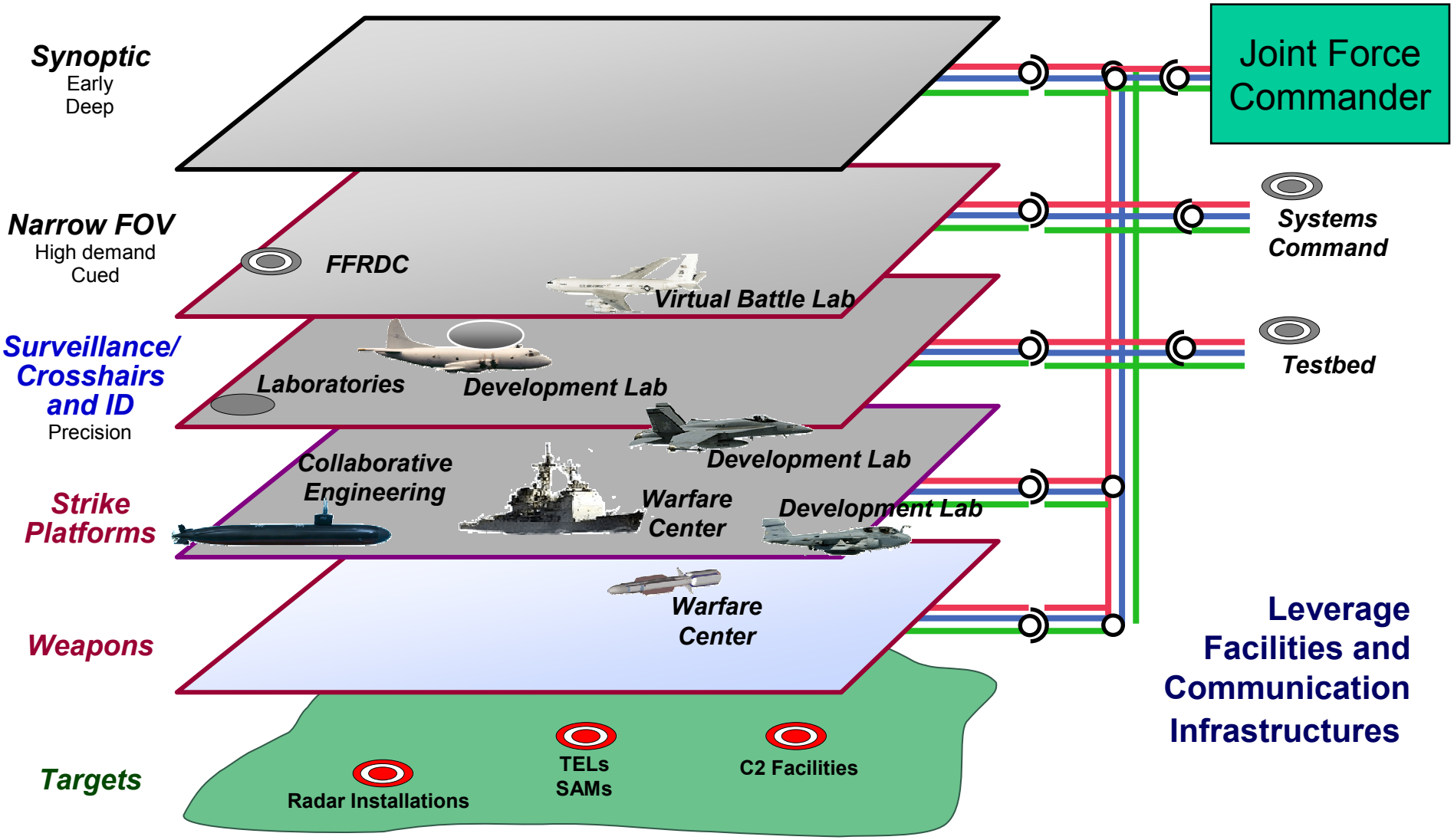
- **End-to-End Force Level System Engineering**
  - Experimentation to resolve issues that needed to be solved
- **Testing Reusable Component Effects across systems and domains**
- **Foster Team work and common understanding across domains**
- **Use Open/Collaborative Engineering Environment across Navy Enterprise**
  - **Leverage existing Netted environments of Land based Test Sites and Live Assets (Via Sea Trial Process) where applicable**
    - Hook up Labs and Fleet connectivity only as needed–Leverage existing facilities and networks
  - **Data Repository/Tools – Enterprise Level Engineering Assessment Capability**
    - Leverage existing tools (e.g. ASN RDA CHENG/NCEE,…) and processes (such as CBM and Business Case Analysis) where applicable

Operational Context View
The Net-Centric Lattice Strike Example

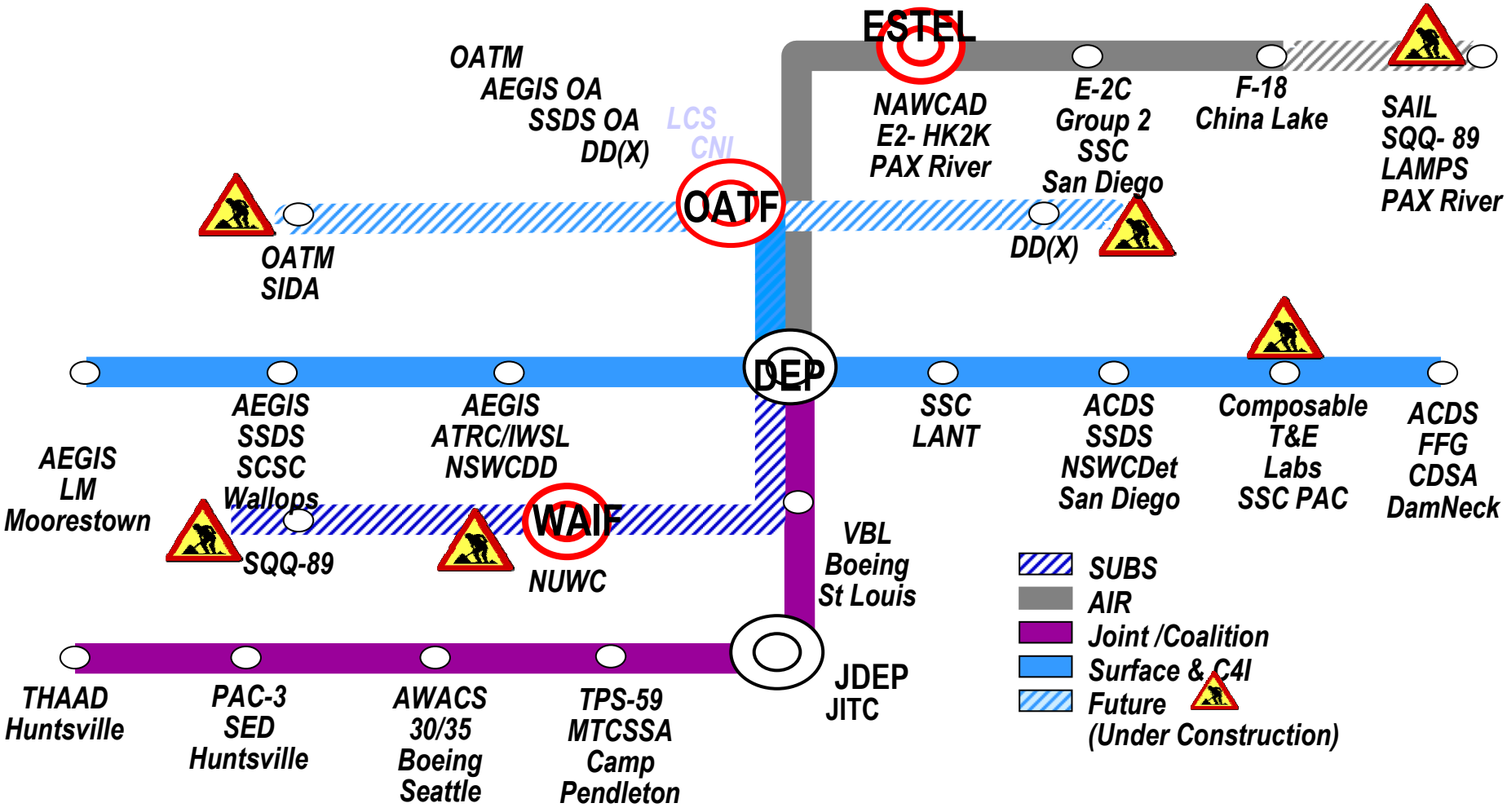


Land-based Test Sites Connectivity View

The Net-Centric Lattice Strike Example

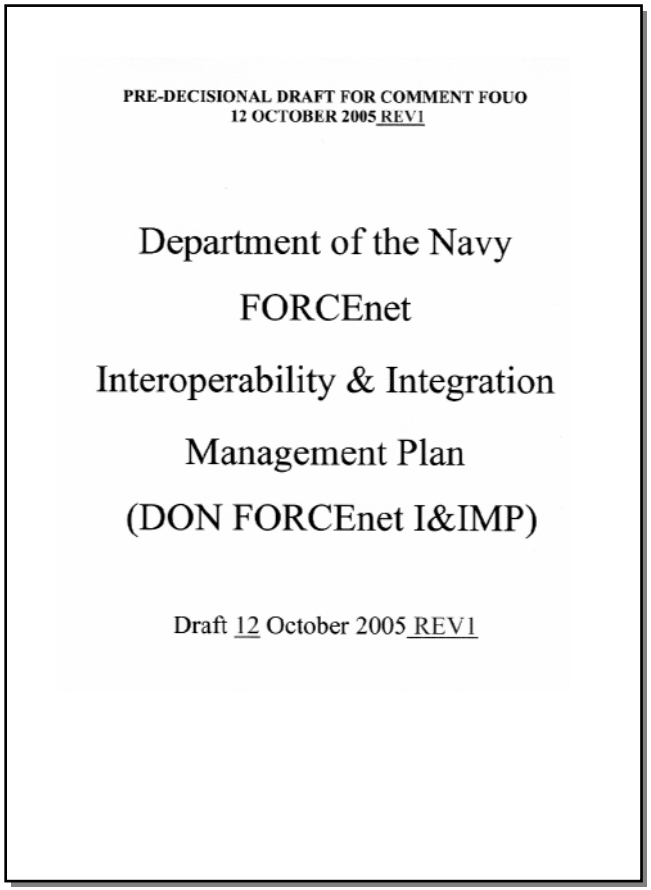


… through a OA / FORCEnet risk reduction experimentation initiative



Transformation Through Collaboration

FORCEnet Integration & Interoperability Management Plan



PRE-DECISIONAL DRAFT FOR COMMENT FOUO
12 OCTOBER 2005 REV1

Department of the Navy

FORCEnet

Interoperability & Integration

Management Plan

(DON FORCEnet I&IMP)

Draft 12 October 2005 REV1

Purpose:

- Establish a management structure and plan for managing I&I of FORCEnet Systems
- Describe procedures, processes and authorities within acquisition community for cooperative design, development, testing and fielding of FORCEnet Systems
- Provide material foundation for capabilities in FORCEnet Functional Concept

Status: In preparation – estimated completion date Mar 06

Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of System Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- **The Technical Cooperation Panel – Technical Panel 4**
- Naval Force Development System

TTCP-JSA-TP4 Terms of Reference

A Technical Panel under Joint Systems and Analysis Group of TTCP

Scope: *Review and exchange best practice and latest research in the application of systems engineering to the enterprise of Defence.*

Vision: *Shape national acquisition strategies and practices to result in effective joint and coalition capabilities.*

TP-4 Status

- Shared the Naval Capability Evolution Process Guidebook with participating countries
- Established a prototype Coalition Collaborative Engineering Environment (CCEE) based on NCEE
- Initiated development of a Coalition Systems Engineering Demonstrator Project

Topics

- Virtual System Commands
- ASN (RDA) Policy for Systems Engineering Plan
- Software Acquisition: Best Practices
- System / System of System Safety
- Naval Capability Evolution Process
- FORCEnet / Open Architecture Integration and Interoperability
- The Technical Cooperation Panel – Technical Panel 4
- **Naval Force Development System (NFDS)**

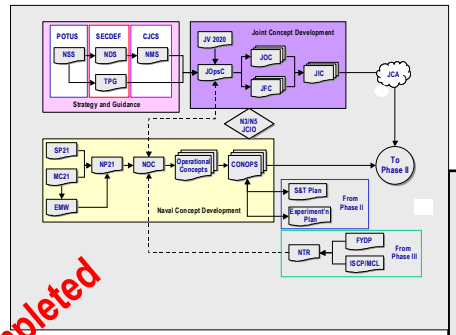
NFDS Objectives

- Capture the "as is" state of the Navy and Marine Corps capability definition, budgeting, and acquisition decision processes and to determine process owners within each of the frameworks
- Identify gaps, overlaps, and misalignments in the services' processes, as well as intersections of the services' methodologies
- Provide a basis for implementing corrective actions to fill gaps, correct misalignments, and improve overall efficiency through greater alignment of processes and commonality of products
- Support senior Navy and Marine Corps leadership to better align naval processes with evolving OSD and Joint Staff transformation to joint capabilities-based investment decisions

Promote informed decisions at all levels

NFDS Status

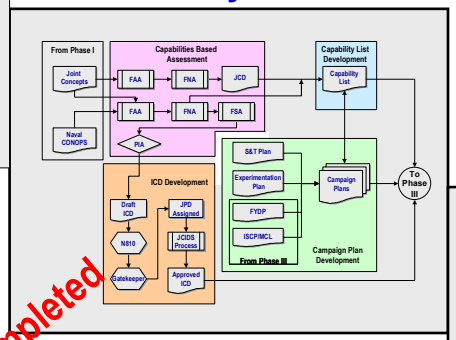
Phase I – Concept Development



Completed

- Operational Concepts
- Warfighting CONOPs

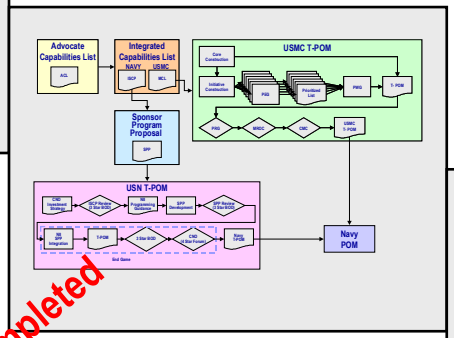
Phase II- Capability Analysis



Completed

- ICD
- Capability List
- Campaign Plans

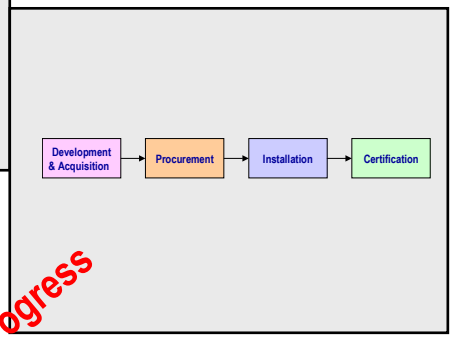
Phase III - Capability Prioritization & Resourcing



Completed

- Advocate Requirement List
- ISCP
- Validated POM
- Etc

Phase IV - Capability Acquisition, Fielding & Transition



In Progress

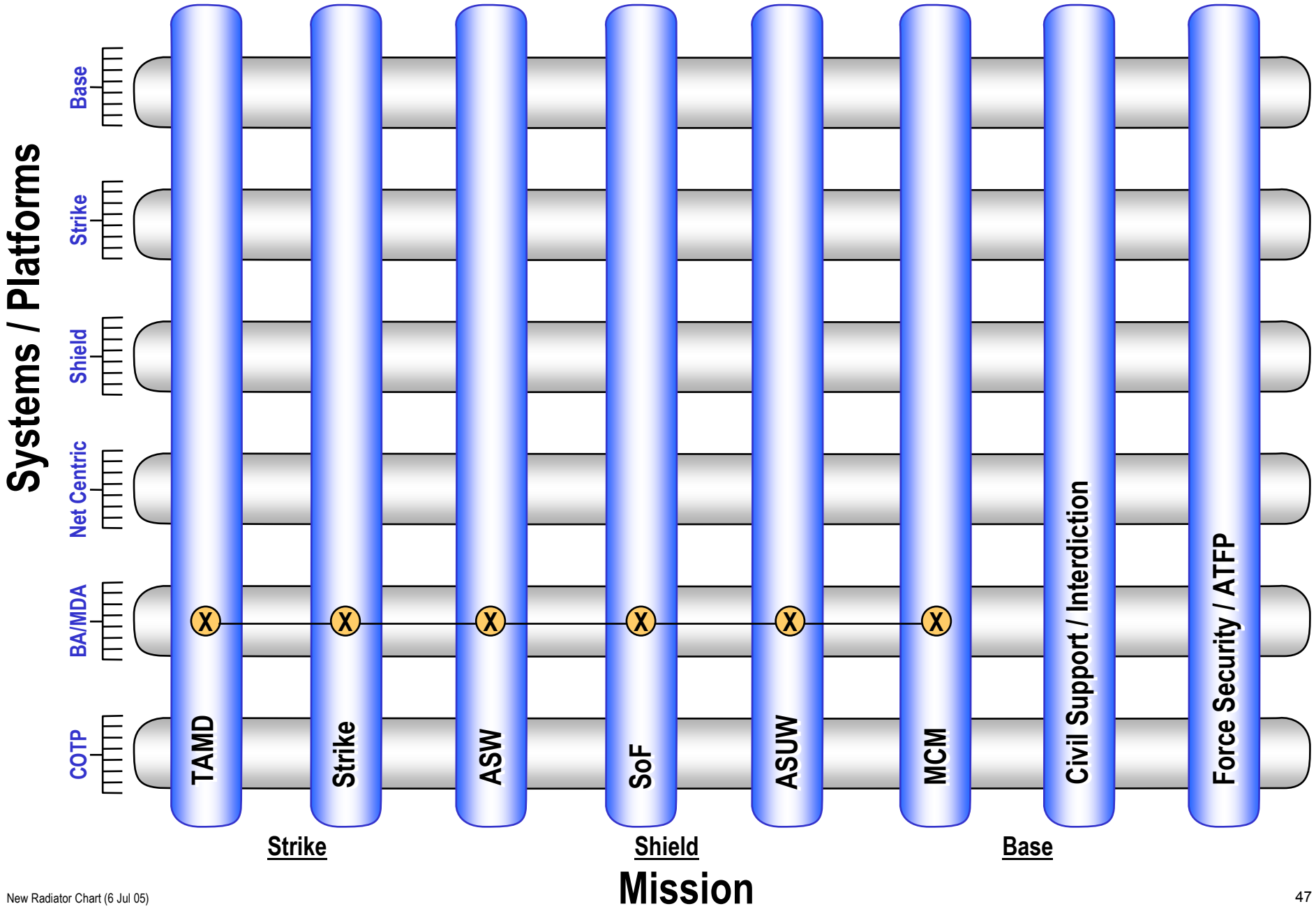
- Acquisition Baselines
- Capability Evolution Document
- Fielding Plans
- Etc

Recommendations

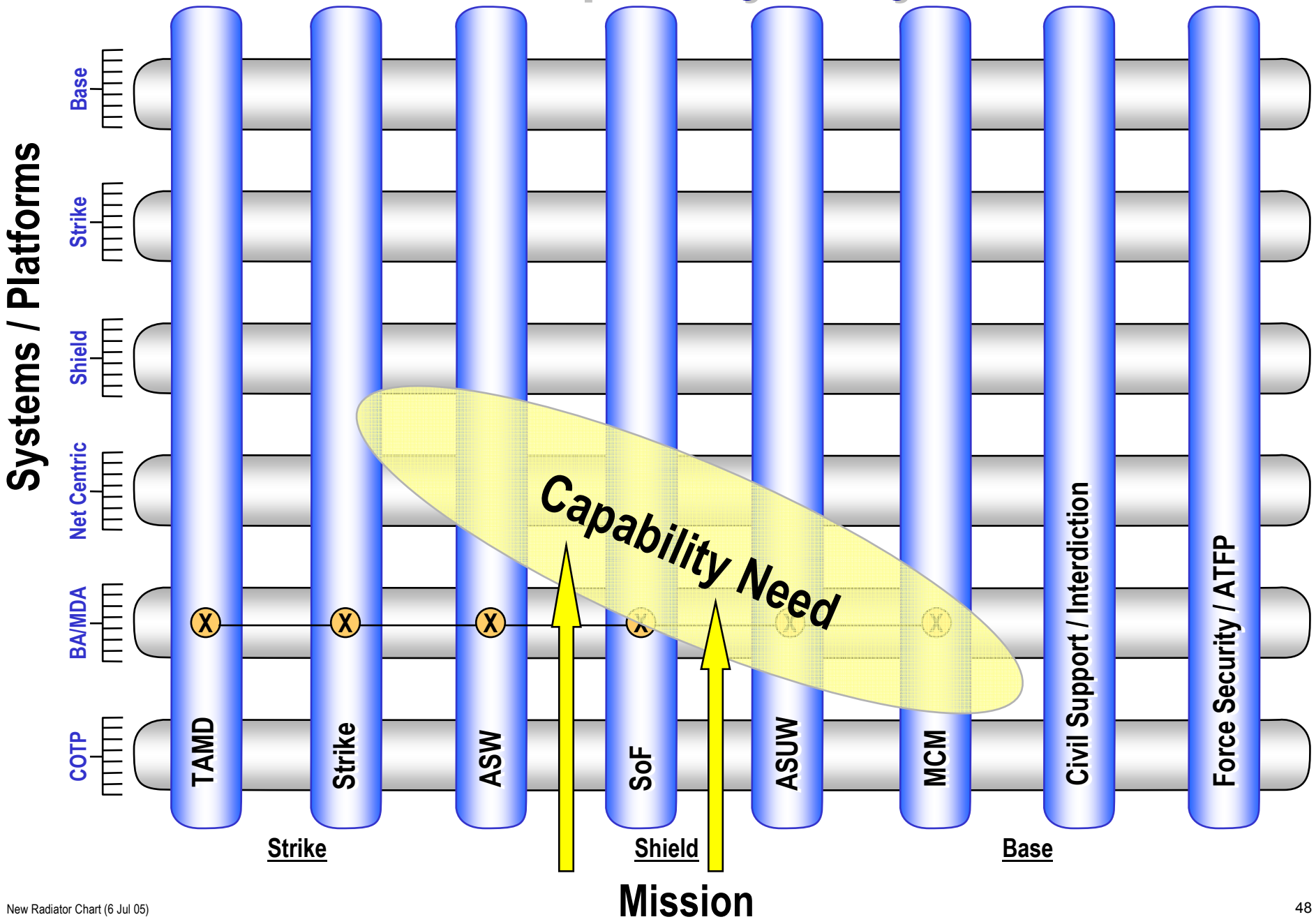
- Formalize enterprise level stakeholder participation among OPNAV, the Fleet, S&T, Acquisition and Secretariat communities
  - Align acquisition community with OPNAV staff to facilitate coordination
- Assign overall concept development responsibility and complete development of Naval concepts
- Implement a Naval Architecture Development and Governance Process
- Designate capability advocates
  - To develop, maintain, and publish capability campaign plans
  - To generate and maintain a required capabilities list as basis for capability gap analysis and POM programming recommendations
- Establish a core POM to improve program stability

Establish Stability, Continuity, and Ownership

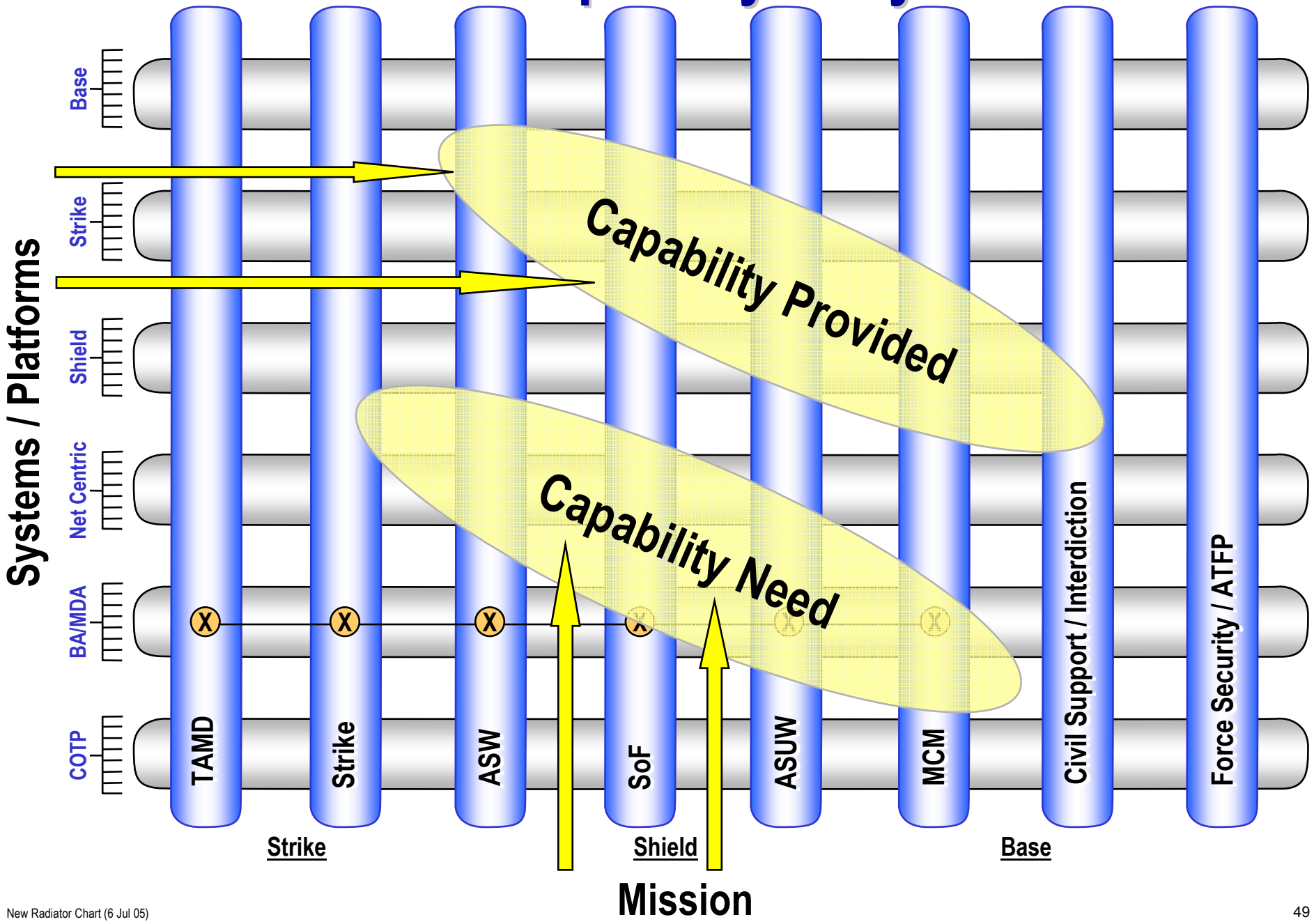
Mission to Capability to System



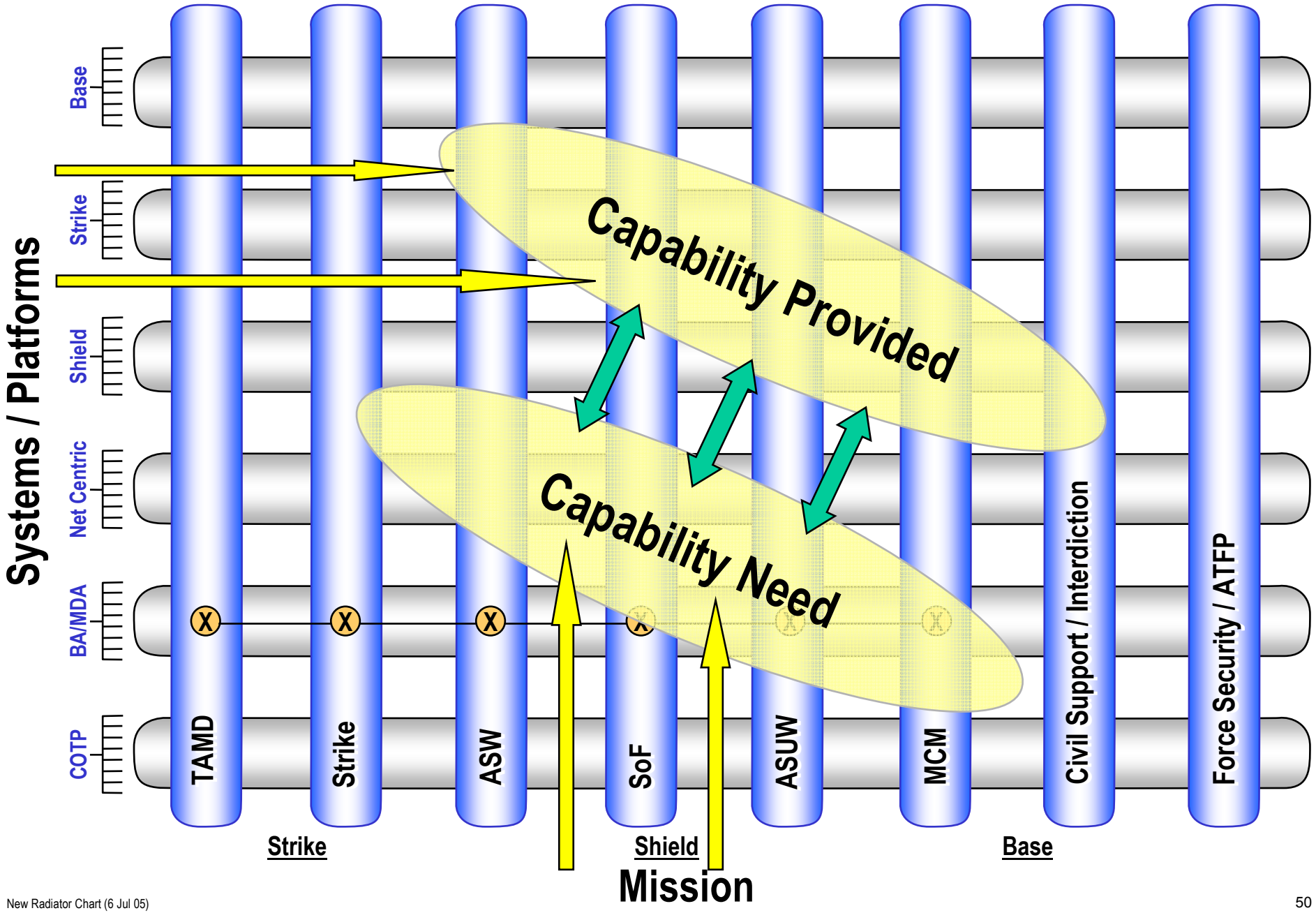
Mission to Capability to System



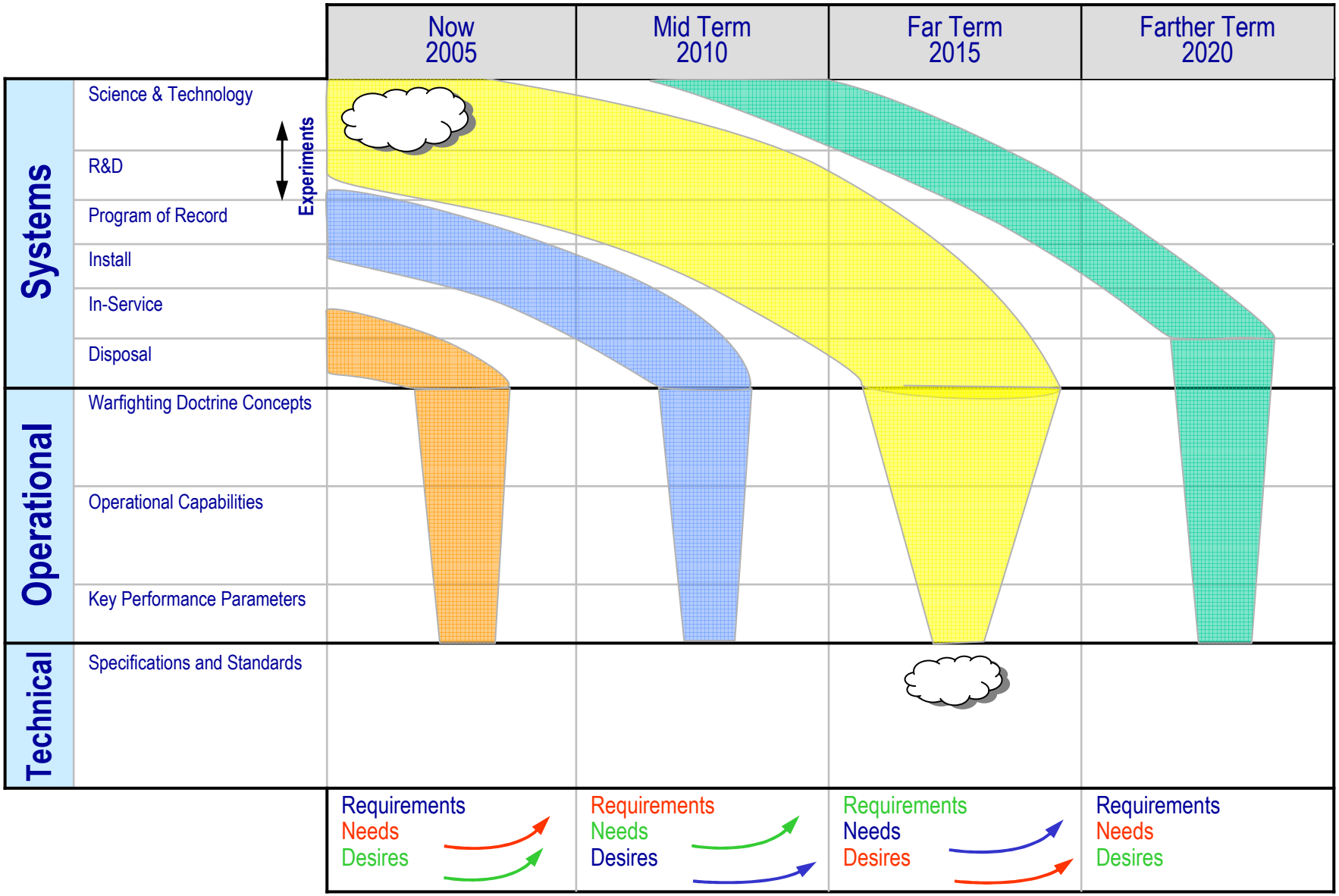
Mission to Capability to System



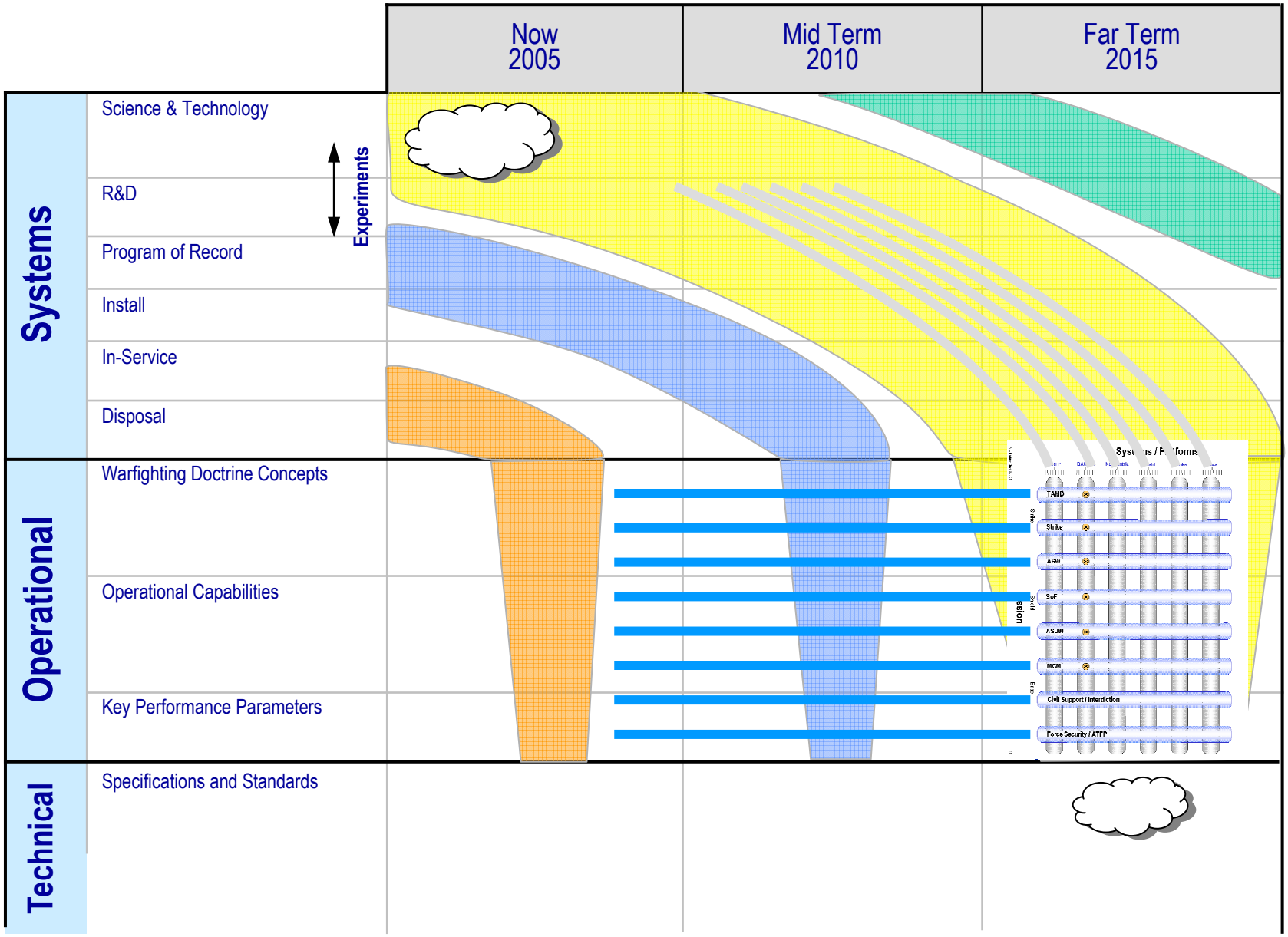
Mission to Capability to System



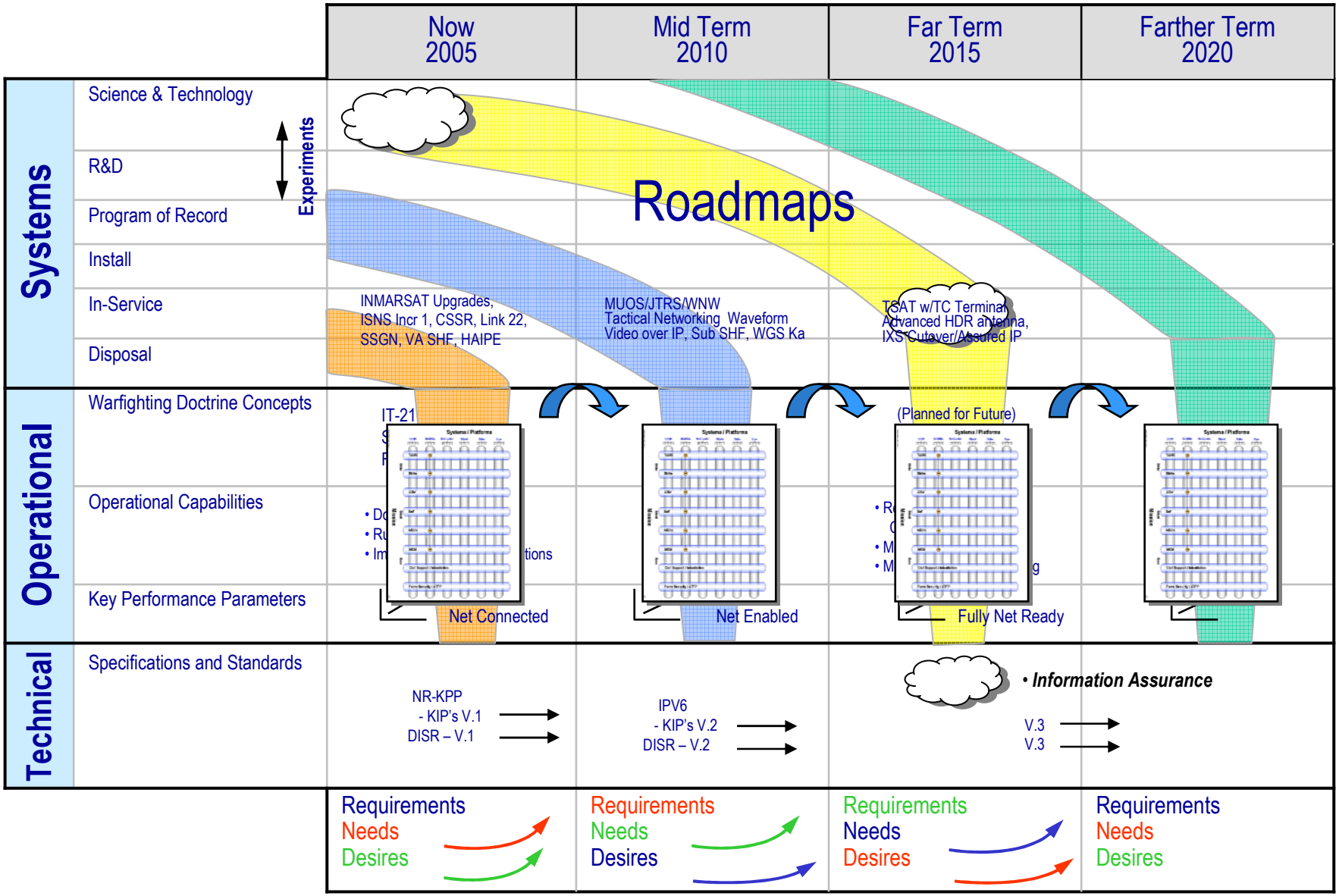
Framework for the "Plan"



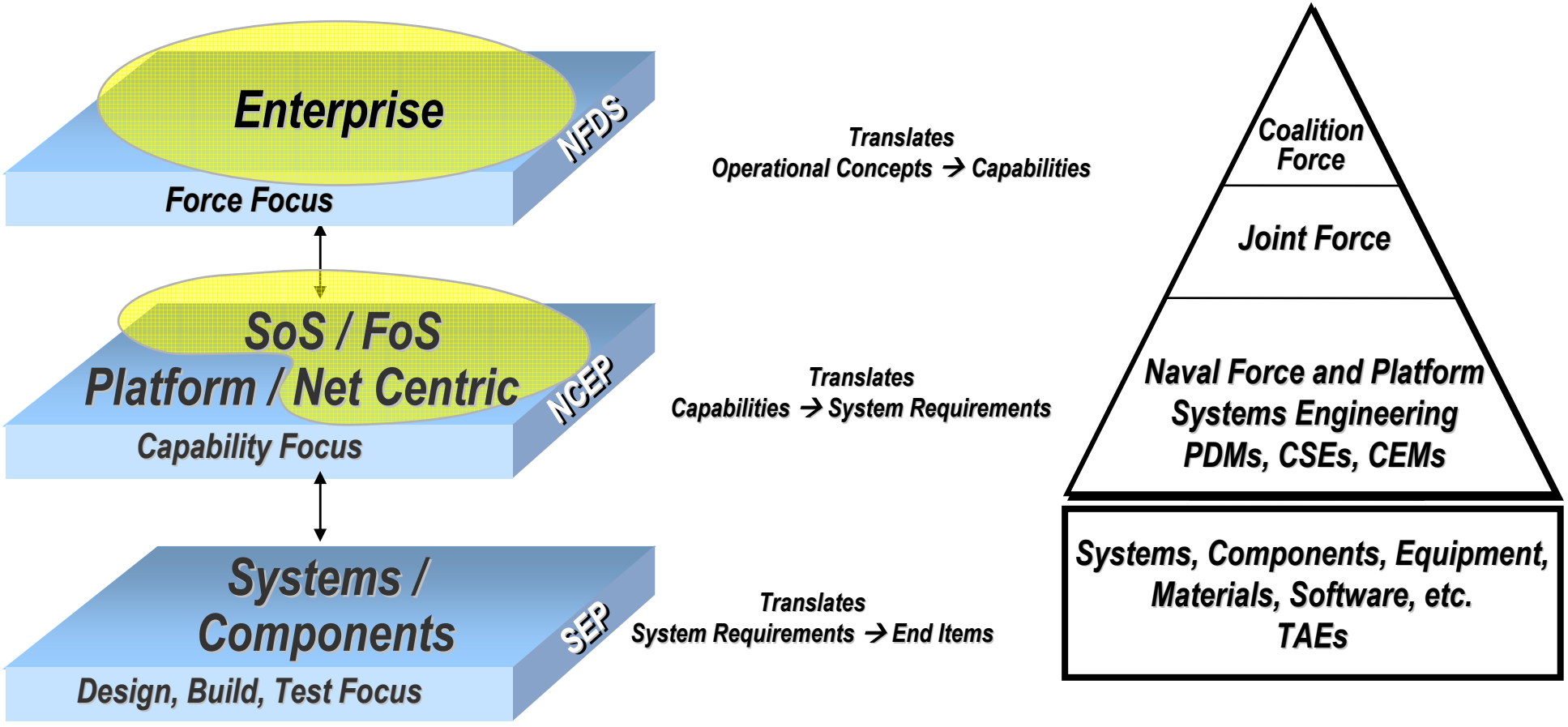
Framework for the "Plan"



Executing the "Plan"



Capability-Based System Engineering



Requires Alignment of Multiple Processes, Process Owners and Products

Backup