Enabling Plug & Fight Capability through
Secured Integrated Networks of Modular, Service Oriented and Open Architectures
(Plug & Fight Architectures)

Cyrus Azani
OSJTF/NGC

SE Conference October 26, 2005
Agenda

- Assumptions
- What is an Open System?
- The Modular Open Systems Approach Principles
- What is Plug and Fight Capability
- The Proposed Strategy
- Guiding Principles for Achieving Net Centric P&F capability
Assumptions Underlying Net-Centric P&F Capability

- Effective Implementation of Existing and Planned DoD-wide initiatives such as:
  - GIG Architecture
  - Information Assurance and Security Infrastructure
  - JBMC2 Roadmap
  - Enterprise Business and Management Architecture
  - DODAF
  - DISR
  - Etc.
- Transparent, Reconfigurable, and Adaptable Architectures and Organizational Structures
- Joint Configuration and Management of Key External Interfaces
- DoD-wide Application of Standardized SE Processes
- Availability of SoS Architecture Modeling Schemes and Standards
Open System: A system that employs modular design, uses widely supported and consensus based standards for its key interfaces, and has been subjected to successful validation and verification tests to ensure the openness of its key interfaces.

MOSA: An integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industry standards organization.
Why Open Systems?

1. **Reduce development cycle** and total life-cycle cost
2. **Enable evolutionary acquisition and spiral development**
3. **Accommodate changing technology and requirements**
4. **Enable access to commercial products from multiple sources both in the initial design and in future enhancements**
5. **Enable affordable interoperability**
6. **Facilitate integration within and among systems**
7. **Enable technology insertion**
8. **Enhance commonality and reuse of components among systems**
9. **Capitalize on modular design tenets**
The MOSA Process

Assess Concepts, Capabilities, Environment & Strategies → Assess Open Systems Feasibility

Establish an Enabling Environment → Develop an Open System Architecture

Employ Modular Design → Use Dynamic Cost Models

Designate Key Interfaces → Use MOSA PART or Equivalent Tools to Assess Progress

Use Open Standards → Use MOSA Contract Lang

Certify Conformance to Standards → Individual Systems and System of System Architects

Designate Key Interface Standards Profiles for Individual Systems and the Joint Mission Capability Areas from Domain Candidates

MOSA Process is Used for development of a Single System as well as System of Systems Architectures
What is Plug & Fight Capability?

- The ability to automatically assemble capabilities/systems/resources and reconfigure them as necessary in response to existing or emerging threats.
- Effectively plug in the needed capabilities/systems and fight without worrying about compatibility, connectivity, and other configuration issues.

*MOSA is the Principal Foundation for Achieving Plug & Fight*
P&F Capability Enablers

- Ability to Quickly Assemble and Reconfigure Forces and Capabilities
  - Adherence to Modular Design Tenets
  - Secured Service Oriented and Open Architectures

- Effective Interface Management
  - Well-defined and Agreed-upon Key Interfaces
  - Continuing Openness Verification and Validation
  - Joint Configuration and Management

- Net Centricity
Achieving the P&F Capability
(A P&F Development Methodology)

1. Employ Modular Design Tenets to Create P&F Mission Modules
2. Designate Key Interfaces for the P&F Mission Modules
3. Develop Key Interface Profiles Using Open Standards and Common Data Strategies
4. Test the Conformance/ Compliance (NR-KPP & Open Standards)
5. Configure/Reconfigure P&F Mission Modules Into Networks of Modular, Secured, Service Oriented, and Open Architectures
6. Manage Key Interfaces via Joint Interface Control Working Groups (JICWG)]
Step 1: Employ Modular Design Tenets to Create P&F Mission Modules

- Cohesive
- Encapsulated
- Loosely Coupled
- Re-useable

P&F Mission Module
Step 2: Designate Key Interfaces for each P&F Mission Module (P&F MM)

Key Interface Designation Criteria:
- High technology turn over rate
- Criticality of function
- Ease of integration
- Change frequency
- Interoperability
- Commonality/reuse
- High cost

Key Interface
- Open Standard

Non-Key Interface
Step 3: Develop Key Interface Profiles Using Open Standards and Common Data Strategies

KIP Elements:

- OV and SV Products
- ICDs
- CCM
- Procedures for standards conformance and interoperability testing
Step 4: Test Conformance/Compliance
(NR- KPP & Open Standards Conformance)

Conformance Tests May be Done on the Following Types of Interfaces:

- Mechanical (bolts, fasteners, connectors and plugs, etc.)
- Fluid (hydraulic, water, etc.)
- Environmental (thermal, nuclear (e.g., neutron, gamma, beta transmission rates and densities), etc.)
- Envelope (space allowances)
- Electrical (power, signals, etc.)
- Sequencing/Programming and timing
- Functional (data formats, etc.)
5. Configure P&F Mission Modules into Ad-hoc Networks

(Joint Warfighting Capability Architecting)
Step 5 Continued…. Networks of P&F Architectures
Constellation of P&F Architectures

US Forces

Open key Interfaces

Allied Forces

Coalition Forces
Step 5 Continued…Integration with Other Architectures
6. Manage Key Interfaces via Joint Configuration Management Councils or Joint Interface Control Working Groups (JICWGs)
2. Designate Key Interfaces for the P&F Mission Modules

1. Employ Modular Design Tenets to Group Systems/Capabilities into P& F Mission Modules

6. Manage Key Interfaces via ICWGs and JCMGs

3. Develop Key Interface Profiles Using Open Standards and Common Data Strategies

4. Test Conformance/Compliance (NR-KPP & Open Standards)

5. Configure P&F Mission Modules into Networks

Conformance Tests May be Done on the Following Types of Interfaces:
- Mechanical (bolts, fasteners, connectors and plugs, etc.)
- Fluid (hydraulic, water, etc.)
- Environmental (thermal, nuclear (e.g., neutron, gamma, beta transmission rates and densities), etc.)
- Envelope (space allowances)
- Electrical (power, signals, etc.)
- Sequencing/Programming and timing
- Software (data formats, etc.)

Key Interface Analyses

Architectural Characteristics

Integration Test Environment

Configuration Management Requirements
Capability Based Assessment (FAA, FNA, FSA, PIA) → DOTMLPF Changes ICD, CDD, CPD (NR-KPP) → Develop Secured Integrated Networks of Service Oriented, Modular, and Open Architectures (Plug & Fight SoS Architectures) → Automated Identification and Resource Allocation Mechanisms

SoS Architecture Development and Modeling Schemes → Automated Identification and Resource Allocation Mechanisms

Modeling Standards → Automated Identification and Resource Allocation Mechanisms

New DODAF Products → Automated Identification and Resource Allocation Mechanisms

Policy Documents NCOW-RM → Automated Identification and Resource Allocation Mechanisms

DISR → Automated Identification and Resource Allocation Mechanisms

DODAF → Automated Identification and Resource Allocation Mechanisms

Automated Identification and Resource Allocation Mechanisms → KIPs Updates

KM/DS → KIPs Updates

Net-Ready Test Certificates → KIPs Updates

KIPs Updates → Net-centric Plug and Fight Capability via Seamless Sharing of Data Among Interconnected Systems and Users

1. Employ Modular Design Tenets to Group Systems/Capabilities into P&F Mission Modules
2. Designate Key Interfaces for the P&F Mission Modules
3. Develop Key Interface Profiles Using Open Standards and Common Data Strategies
4. Test Conformance/Compliance (NR-KPP & Open Standards)
5. Configure P&F Mission Modules into Networks
6. Manage Key Interfaces via ICWGs and JCMGs

MOSA Enabling Environment

Standardized Systems Engineering Process

Joint Configuration & Management

Net-centric Plug and Fight Capability via Seamless Sharing of Data Among Interconnected Systems and Users
A “V” Model for Enabling Net-Centric P&F Capability

INPUTS

- Needed P&F Capabilities
- JCAs
- DODAF Products
- Lessons Learned
- Market Research Findings

OUTPUTS

- New P&F Capabilities
- KIPs updates
- Test Certificates
- Updated DODAF Products

Prepare an Enabling Environment

- Assess the
- Validate enabling
- Conditions

Create P&F mission modules

- Designate key interfaces for P&F modules
- Develop Key interface profiles

Configure P&F Modules into Networks

- Manage key interfaces via JCM teams
- Verify adherence to modular design tenets

Verify the Designation Appropriateness

- Verify conformance
- Conduct trade-off analysis
- Establish metrics and conduct periodic reviews

Integrated Networks of secure, modular, service oriented and open architectures (P&F Architectures)

MOSA Enabling a Standardized SE Environment
Achieving P&F Capability

Networks of Service Oriented, Secured, Reconfigurable, and Open Architectures

Technology
(SoS Engineering, Adaptive Tools, Models, Methods, Standards & Processes)

Culture
(Free Flow of Information, Change in Behavior, Responsive Organizational Constructs, Compatible Semantics & Data Format)

Capability-Based Acquisition
(Ad-hoc Architecting)

Net Centricity Must be Designed into the Systems Rather than be Tested after Development
Empower Program Managers and other Acquisition Personnel to Effectively:

- Provide “plug and fight” capability at all levels in all domains by using transparent systems that can be reconfigured and integrated rapidly
- Address P&F Capability as major required capability and system attributes (AOA, ICD, CDD, CPD, Acquisition Strategy)
- Leverage commercial technology and practices
- Use SoS Engineering to integrate capabilities rather than develop stove-piped systems
- Balance battlefield performance and interoperability with ease of integration and total life cycle affordability
- Provide full logistics supportability via access to multiple sources of supply throughout the systems life cycle
- Modernize systems through incremental upgrades (“modernization through spares” concept)
- Build a fully synergistic partnership among the Services, AT&L, Joint Staff and with the industry.

An integrated network of open and modular architectures is the principal foundation for configuring forces and systems rapidly and affordably
Questions?

Open Systems
Joint Task Force

Please send your comments to Cyrus Azani at cyrus.azani.ctr@osd.mil
Examples of Standards Needed

- **Technical Standards (operational domain independent)**
  - Execution environment standards (POSIX, COM, J2EE, C++, ...)
  - Interaction-based standards (Telephony, TCP/IP, http, ODBC, ...)
- **Information Representation Standards (ebXML, UPC, uucode, ...)**
  - Increasingly operational domain specific; communities of interest
- **Service Standards (SOAP, WSDL, SAML, ....)**
  - Driven by the IT industry and common requirements
- **Standard Services (DNS, UDDI, NCES, Blue Force Tracking, ....)**
  - Driven by “the enterprise”; operational effectiveness
- **Product Standards (FIPS, compliance with other standards)**
- **Standard (Common) Products – primarily “enterprise” cost driven**
- **Specifications – acquisition community oriented**
- **Modeling Standards (Open Model Interface (IEEE 1499), AP33, Etc.)**