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**

Definitions

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.

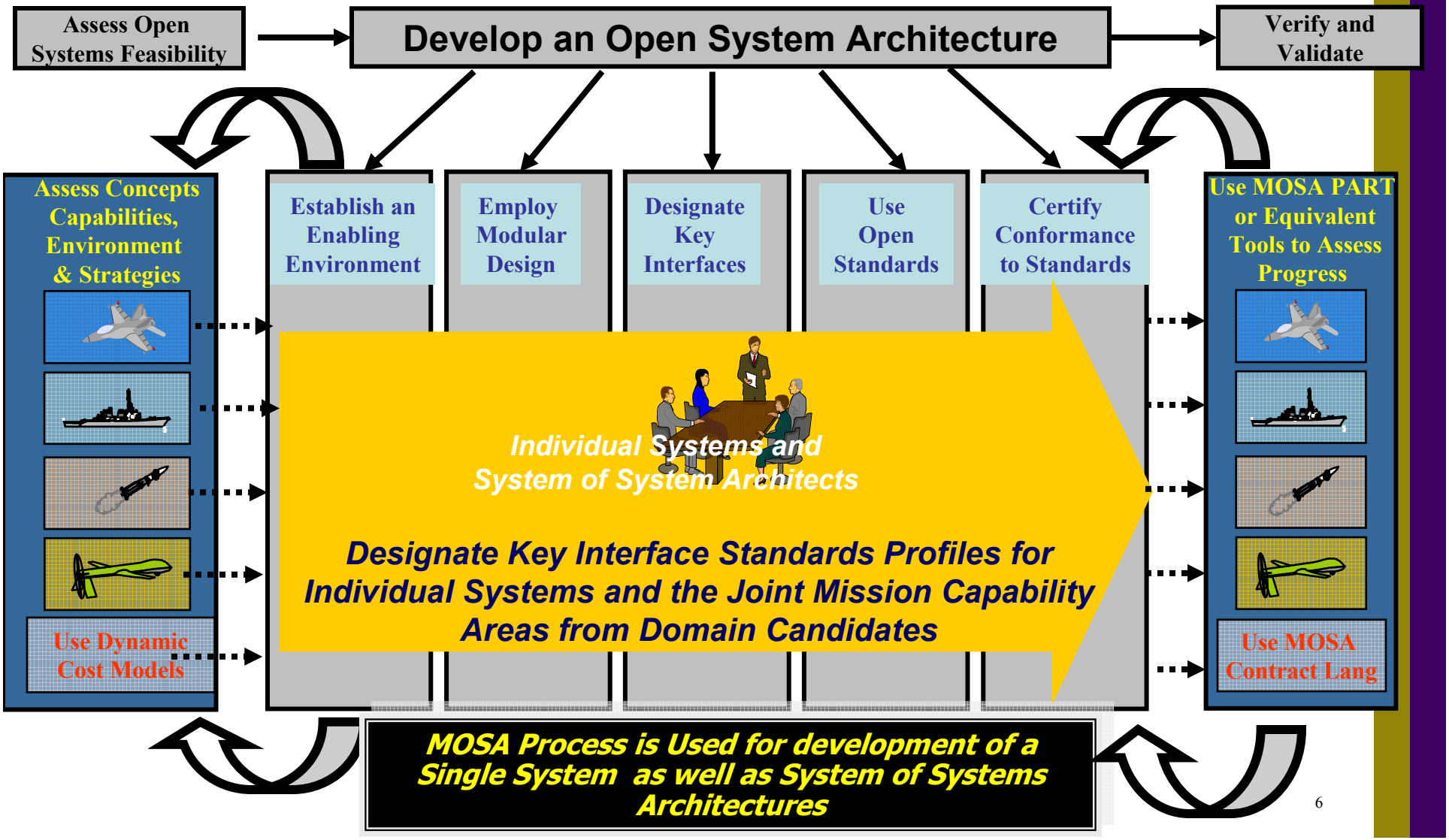
MOSA: An integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industry standards organization.

Why Open Systems?

OPEN SYSTEMS OS JOINT TASK FORCE

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



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

OPEN SYSTEMS OS JOINT TASK FORCE

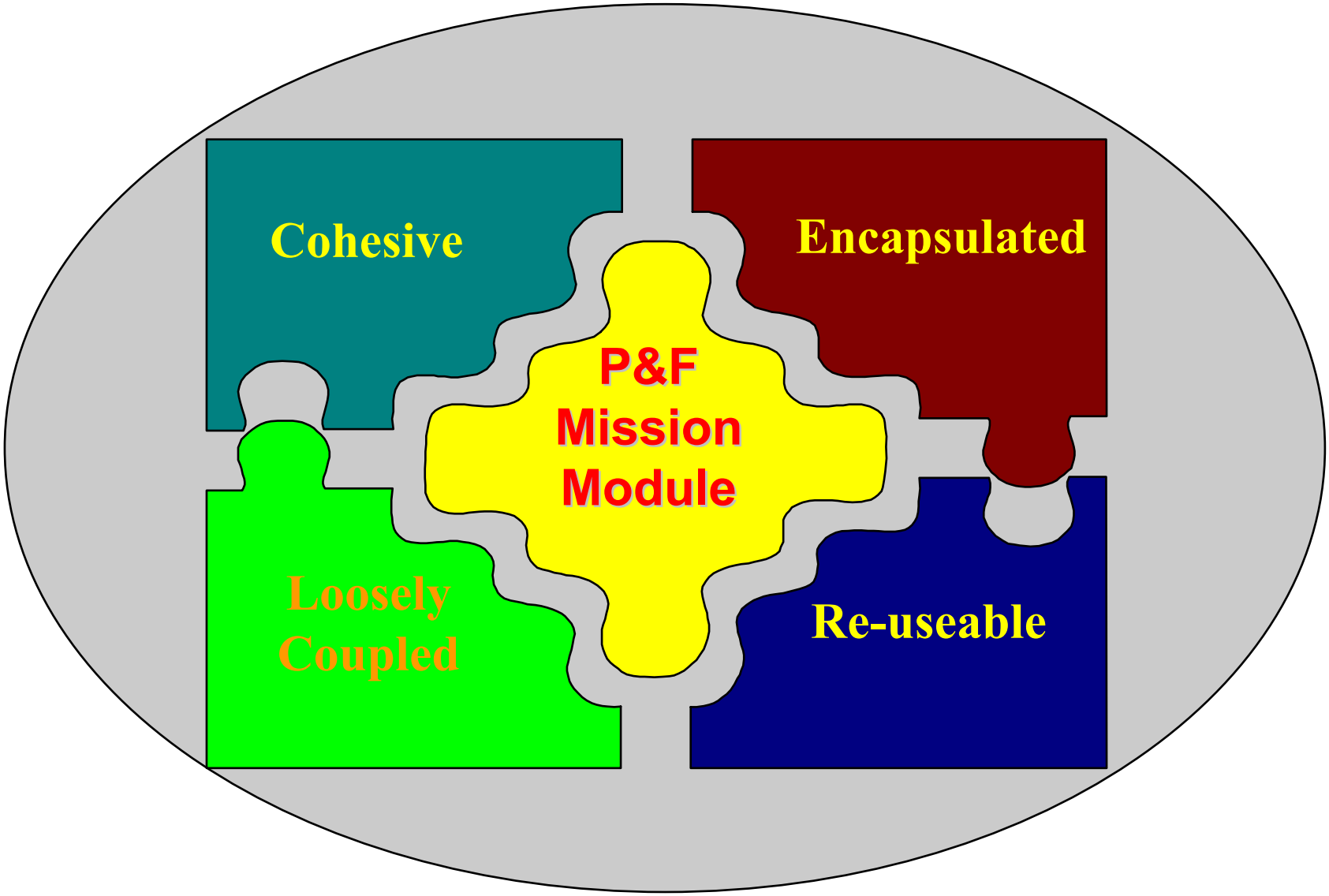
- Ability to Quickly Assemble and Reconfigure Forces and Capabilities
  - Adherence to Modular Design Tenets
  - Secured Service Oriented and Open Architectures
- Effective Interface Management
  - Well-defined and Agreed-upon Key Interfaces
  - Continuing Openness Verification and Validation
  - Joint Configuration and Management
- Net Centricity

Achieving the P&F Capability
(A P&F Development Methodology)

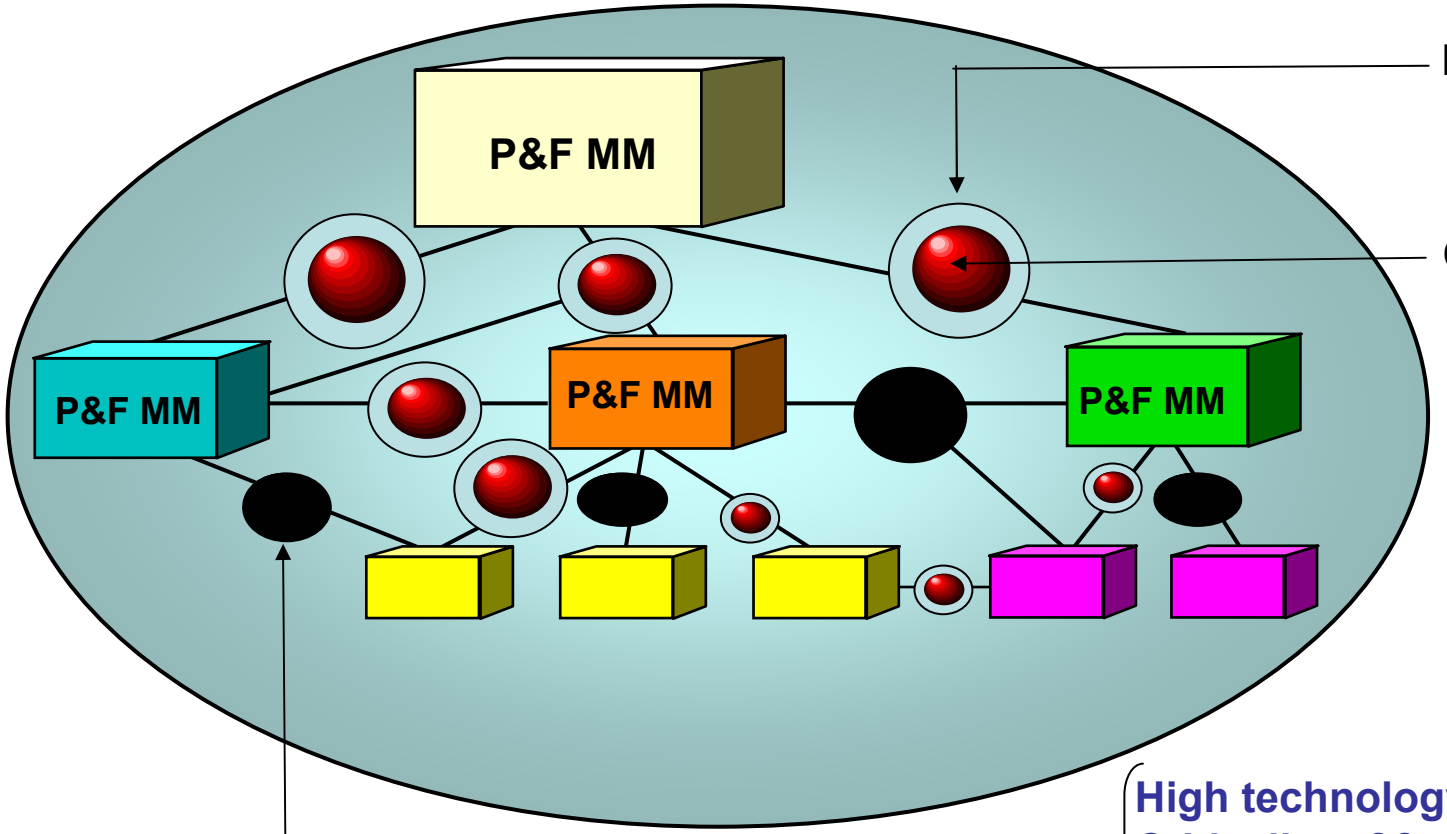
OPEN SYSTEMS JOINT TASK FORCE

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 (JICWGs)

Step1: Employ Modular Design Tenets to Create P& F Mission Modules



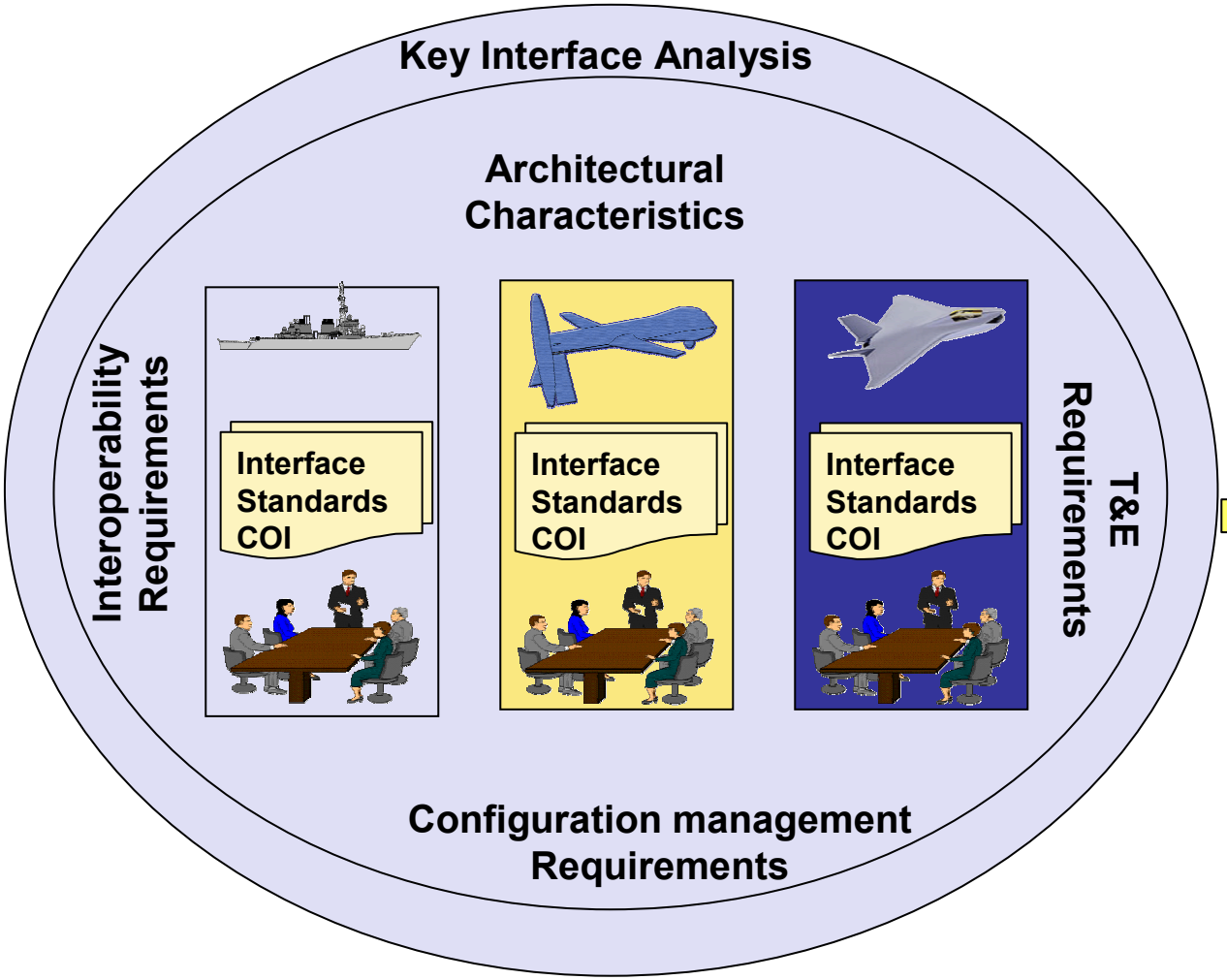
Step 2: Designate Key Interfaces for each P&F Mission Module (P&F MM)



Key Interface Designation Criteria:

- High technology turn over rate
- Criticality of function
- Ease of integration
- Change frequency
- Interoperability
- Commonality/reuse
- High cost

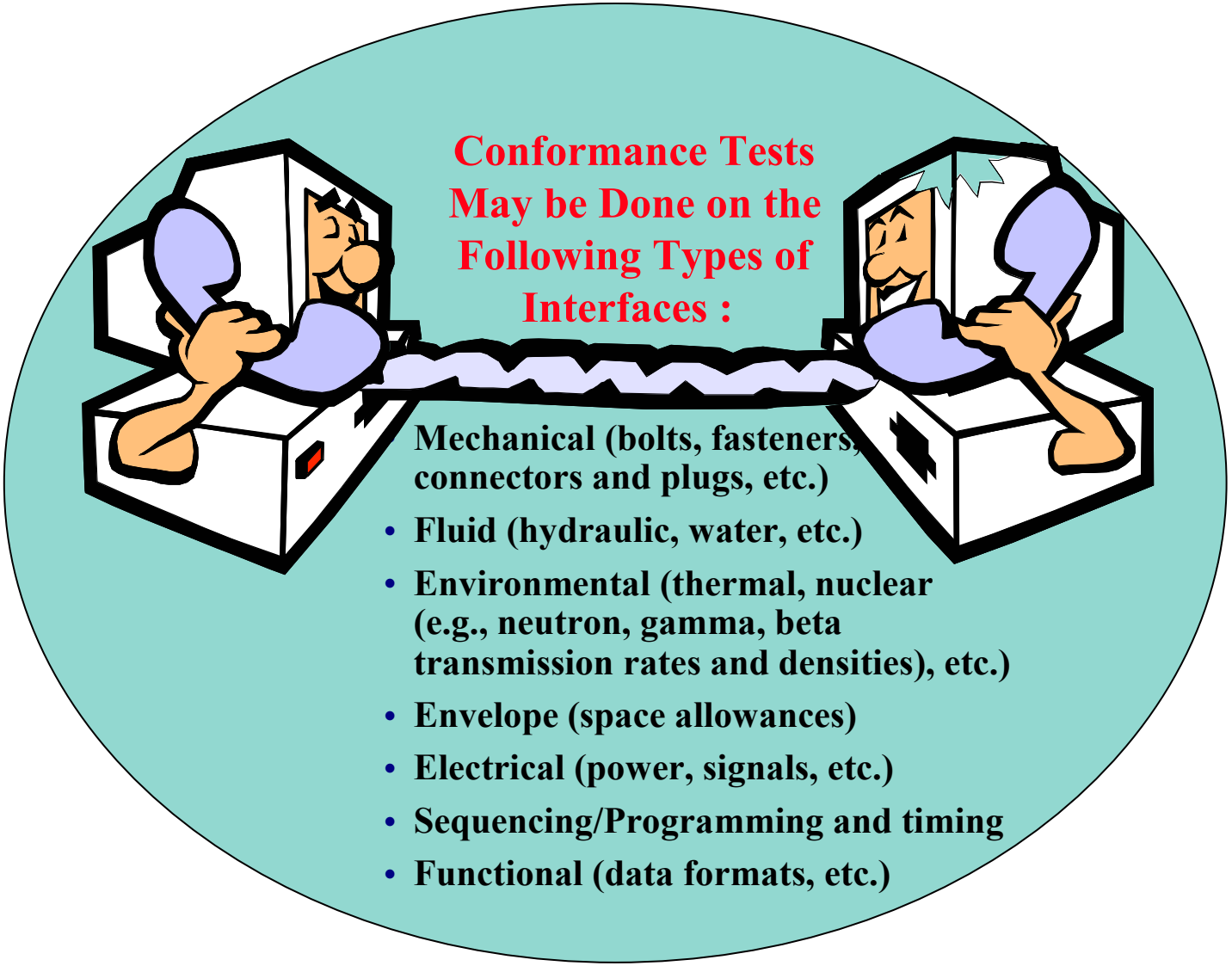
Step 3: Develop Key Interface Profiles Using Open Standards and Common Data Strategies



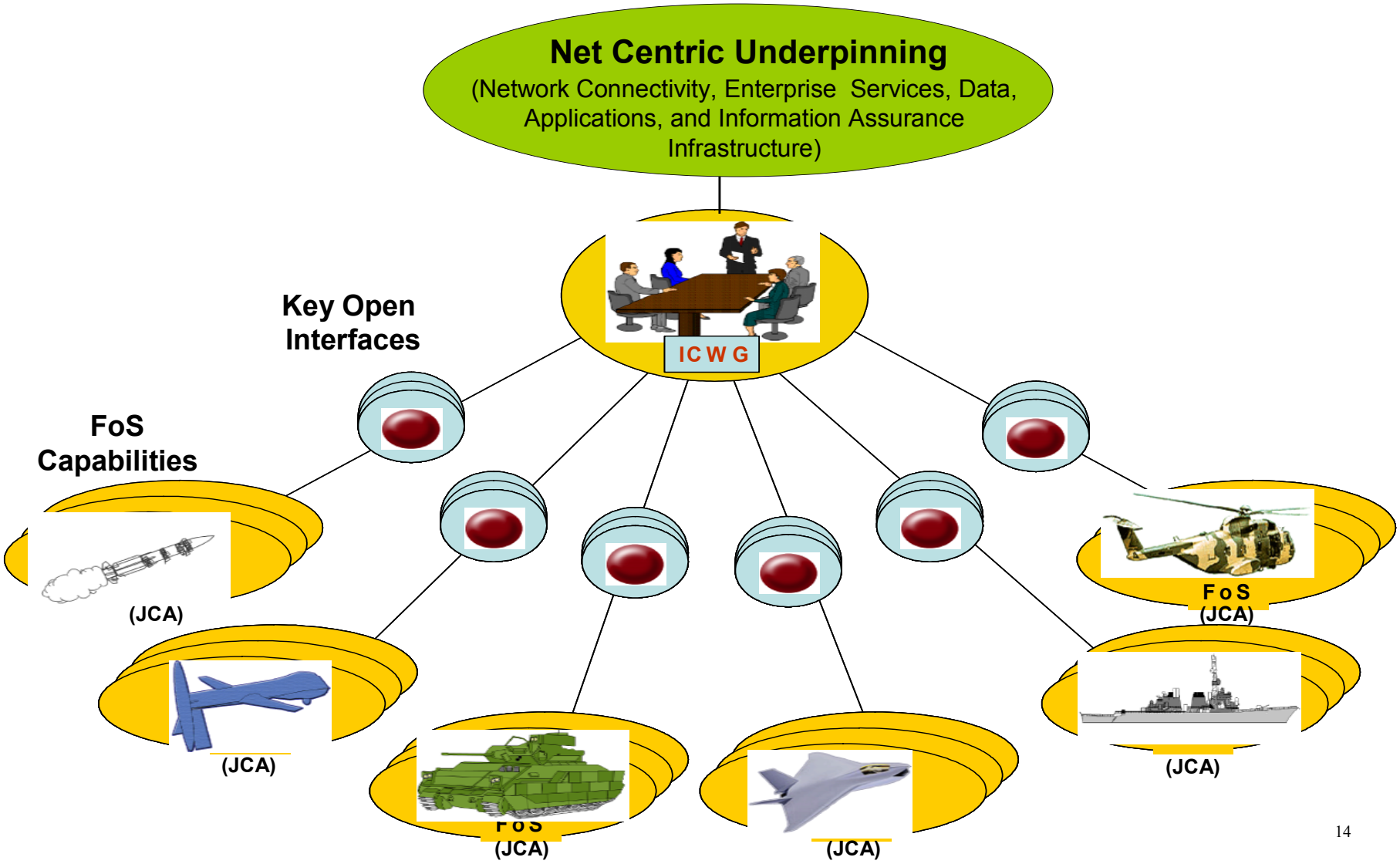
KIP Elements:

- OV and SV Products
- ICDs
- CCM
- Procedures for standards conformance and interoperability testing

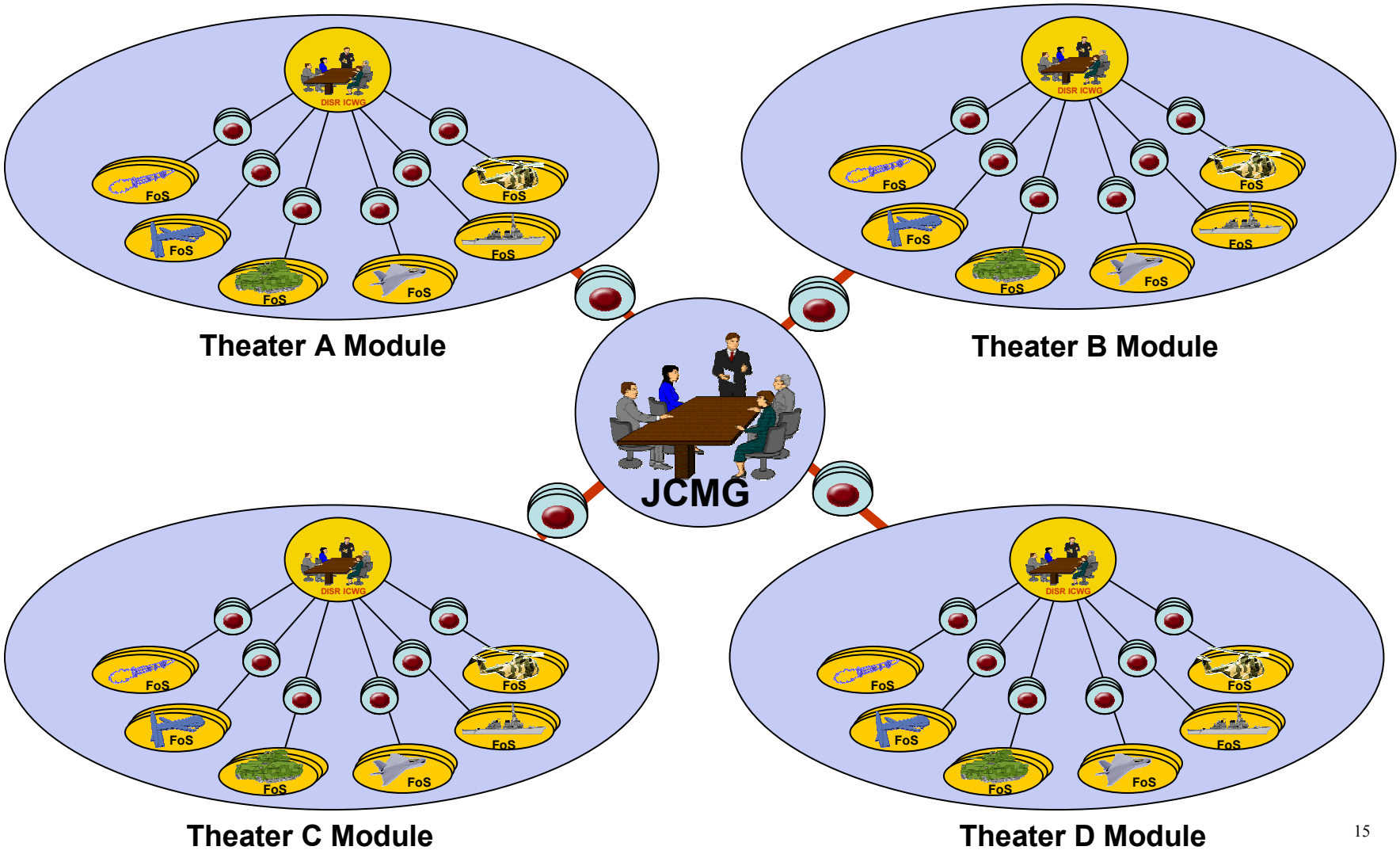
Step 4: Test Conformance/Compliance (NR- KPP & Open Standards Conformance)



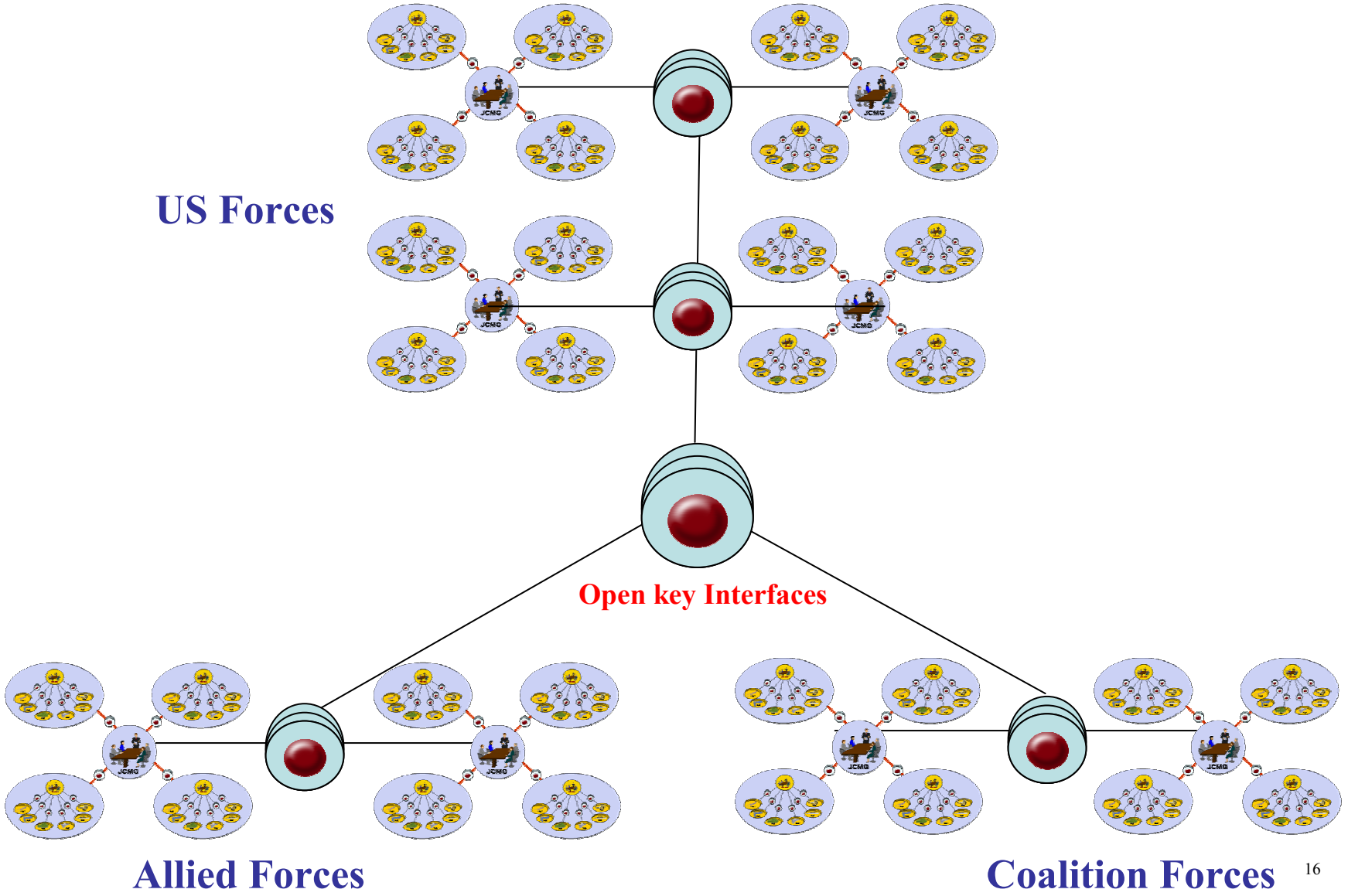
5. Configure P&F Mission Modules into Ad-hoc Networks (Joint Warfghting Capability Architecting)



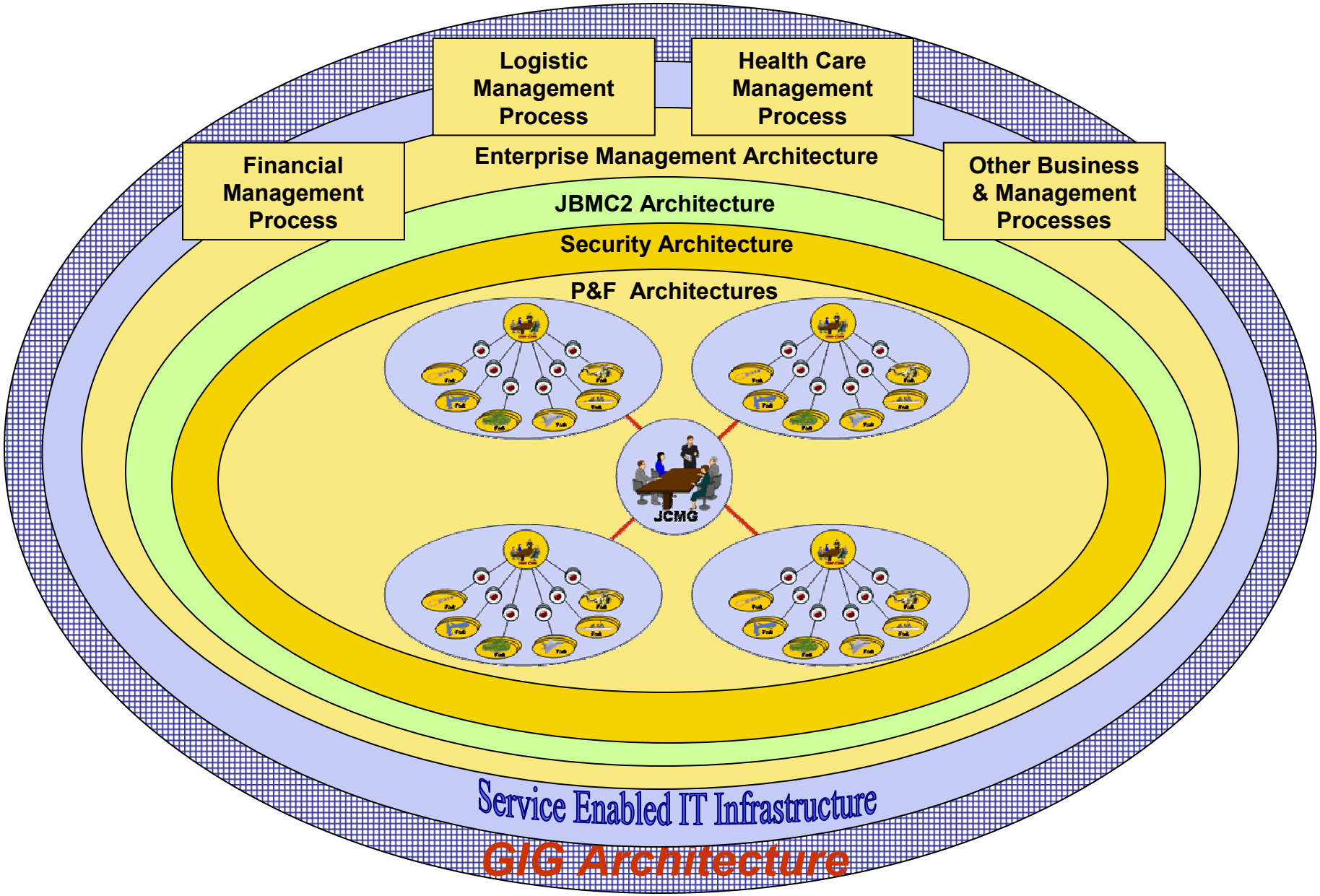
Step 5 Continued…. Networks of P&F Architectures



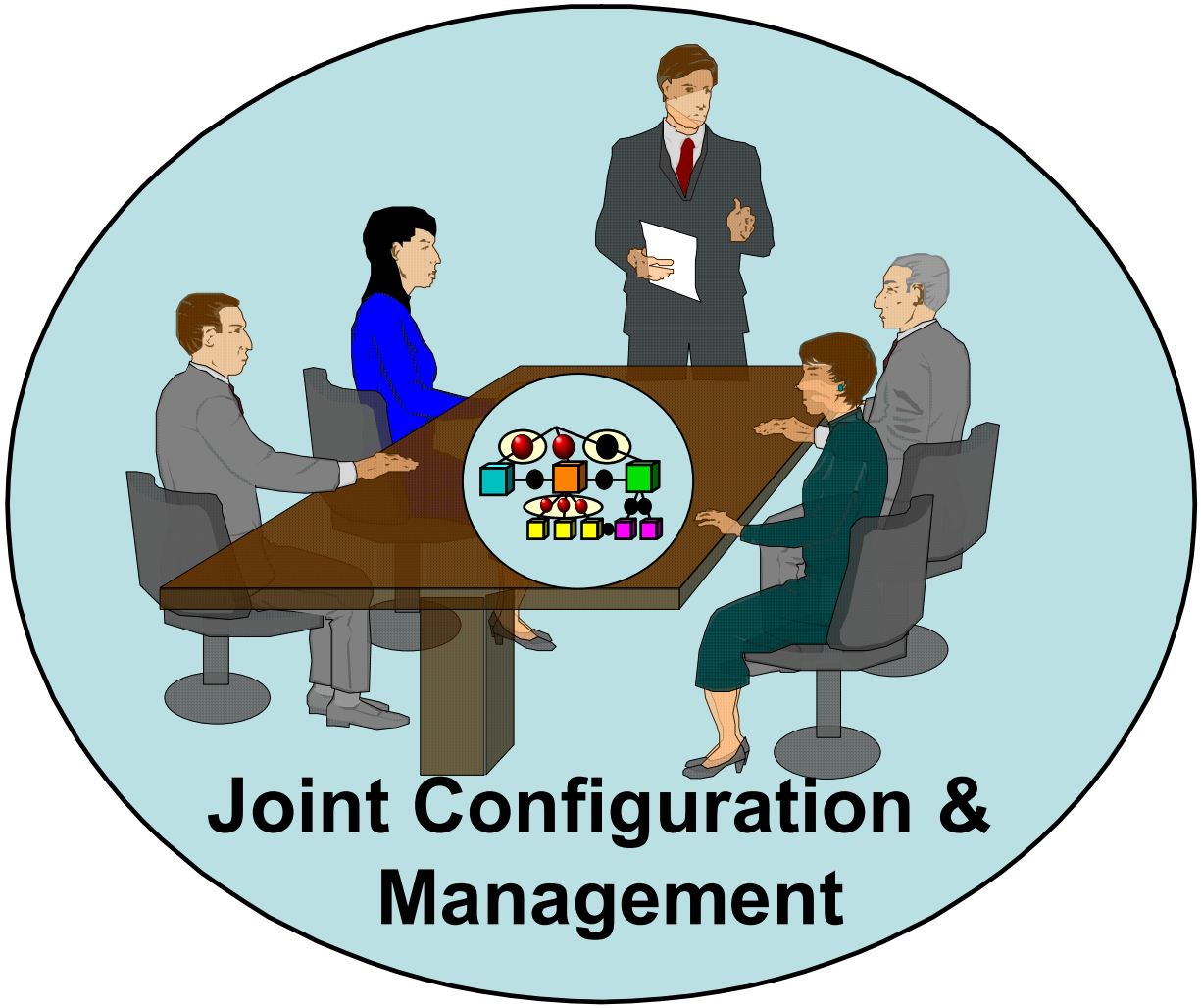
Constellation of P&F Architectures



Step 5 Continued…Integration with Other Architectures

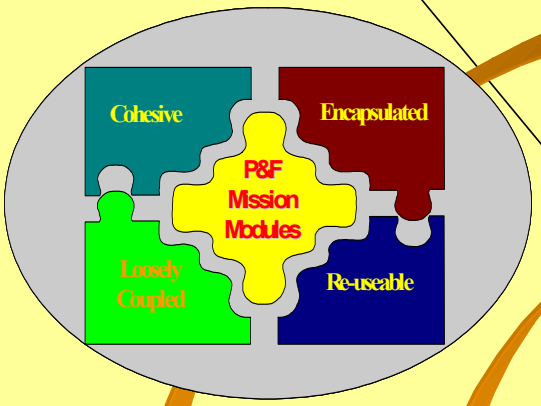


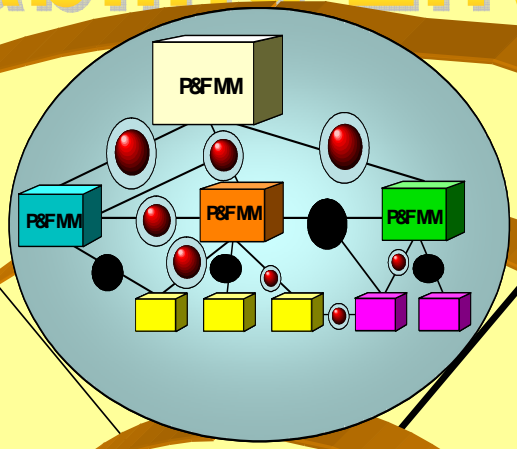
6. Manage Key Interfaces via Joint Configuration Management Councils or Joint Interface Control Working Groups (JICWGs)

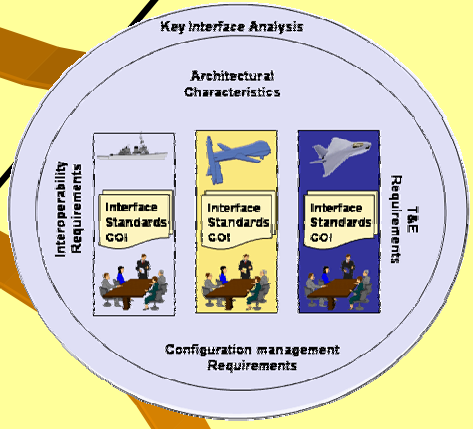


MOSA Enabled Environment

2. Designate Key Interfaces for the P&F Mission Modules





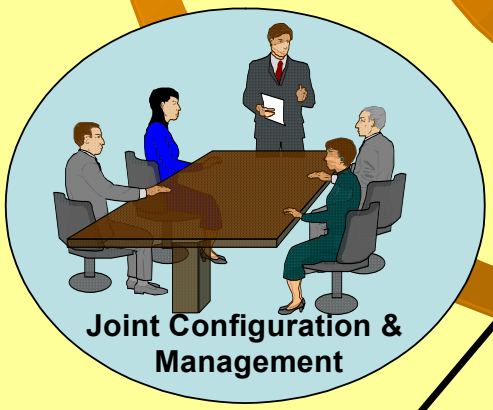


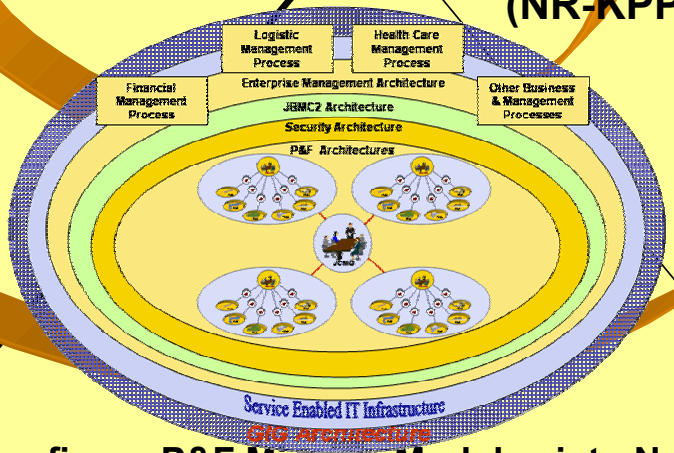
1. Employ Modular Design Tenets to Group Systems/Capabilities into P& F Mission Modules

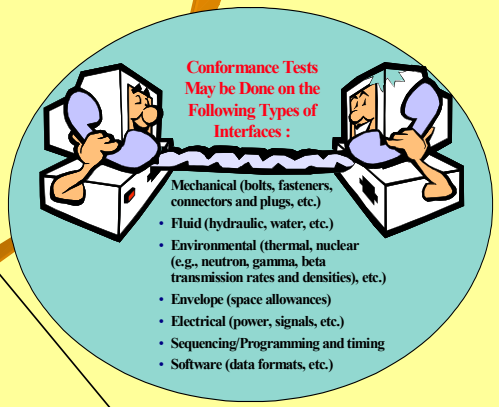
3. Develop Key Interface Profiles Using Open Standards and Common Data Strategies

6. Manage Key Interfaces via ICWGs and JCMGs)

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







5. Configure P&F Mission Modules into Networks

Standardized Systems Engineering Process

Capability Based Assessment (FAA, FNA, FSA, PIA)

DOTMLPF Changes ICD, CDD,CPD (NR-KPP)

Policy Documents NCOW-RM

DISR

DODAF

SoS Architecture Development and Modeling Schemes

Develop Secured Integrated Networks of Service Oriented, Modular, and Open Architectures (Plug & Fight SoS Architectures)

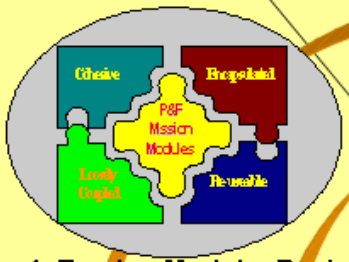
Automated Identification and Resource Allocation Mechanisms

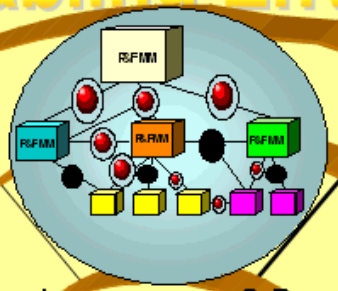
Modeling Standards

KM/DS

MOSA Enabling Environment

2. Designate Key Interfaces for the P&F Mission Modules



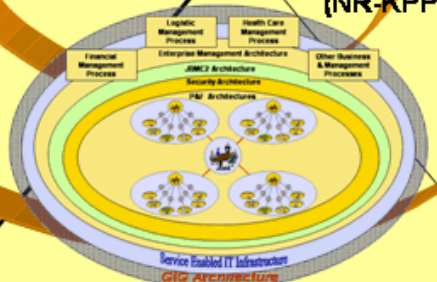


1. Employ Modular Design Tenets to Group Systems/Capabilities into P& F Mission Modules

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

6. Manage Key Interfaces via ICWGs and JCMGs)

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



5. Configure P&F Mission Modules into Networks

Standardized Systems Engineering Process

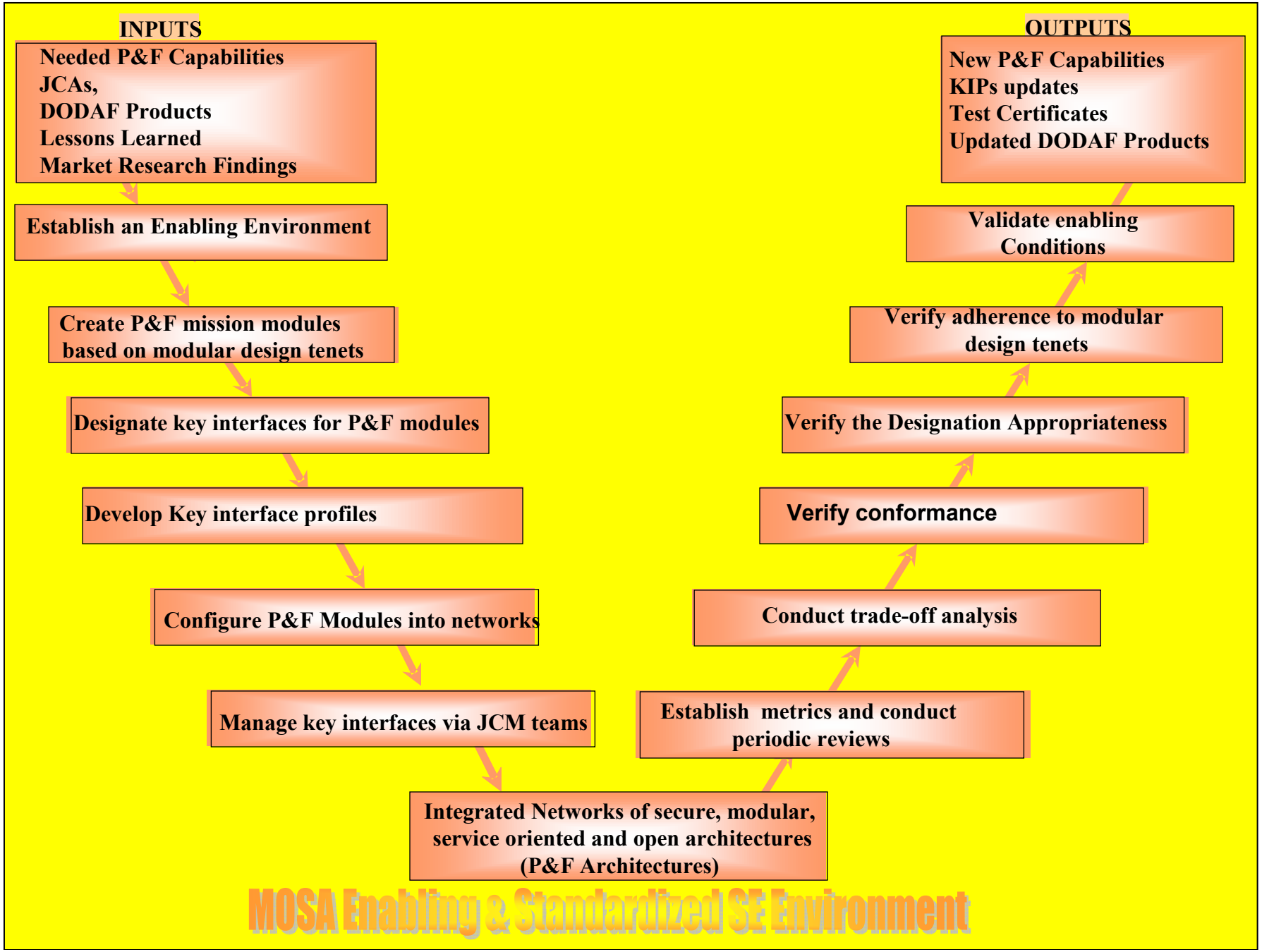
KIPs Updates

New DODAF Products

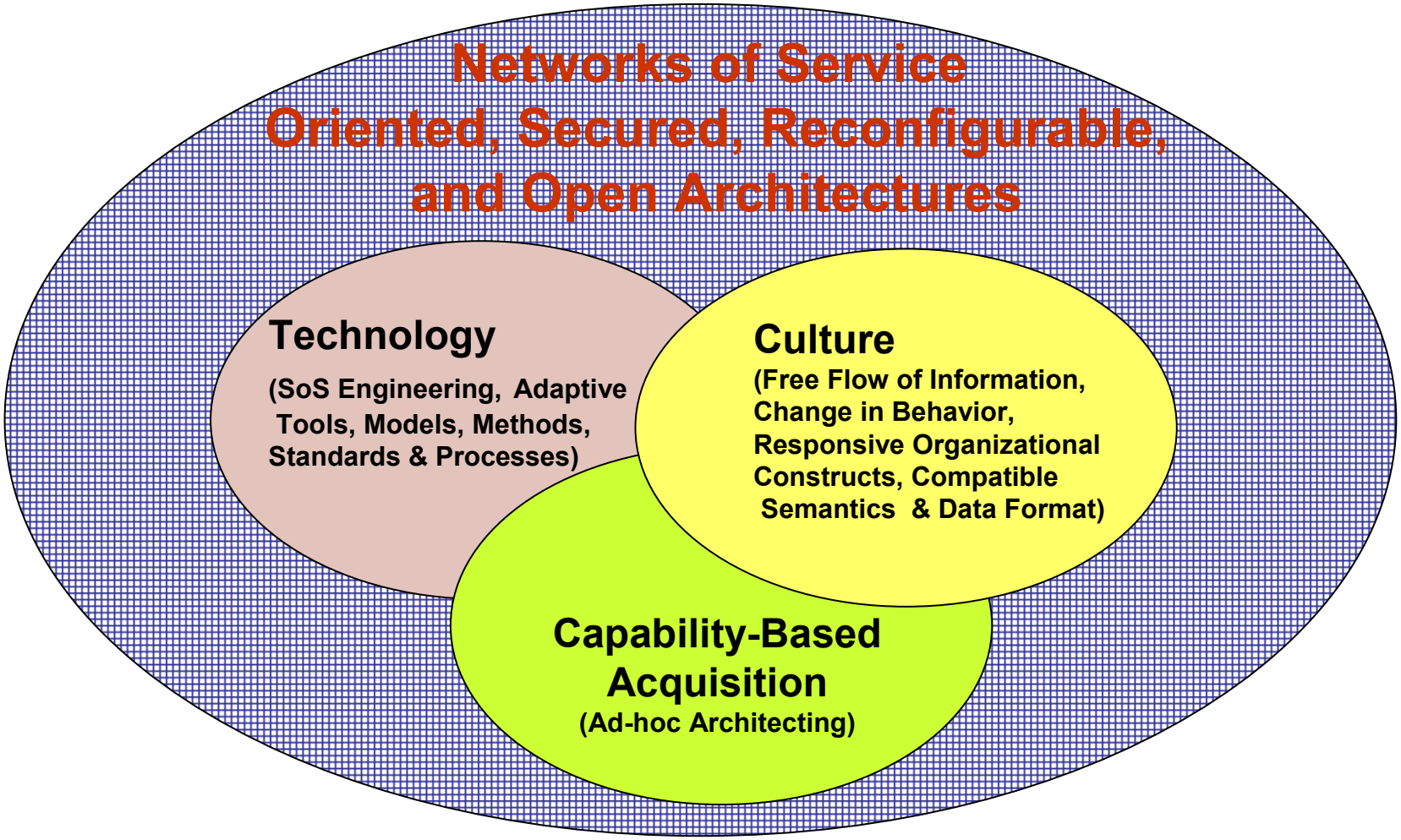
Net-Ready Test Certificates

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



Achieving P&F Capability



Net Centricity Must be Designed into the Systems Rather than be Tested after Development

OPEN SYSTEMS JOINT TASK FORCE

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
OS
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.)