



Counterfeit Prevention in the DoD: A Technical Perspective

Mr. Nicholas M. Torelli

Director, Mission Assurance

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering**

**SAE 2012 Counterfeit Parts Avoidance Symposium
Phoenix, AZ | November 2, 2012**



Systems Engineering



- **To make good acquisition decisions, we need to understand and manage, in a deep way, the myriad technical risks involved in designing, developing and delivering some of the most complex systems ever deployed**
- **Systems Engineering focuses on engineering excellence – the creative application of scientific principles:**
 - To design, develop, construct and operate complex systems
 - To forecast their behavior under specific operating conditions
 - To deliver their intended functions while addressing economic efficiency, environmental stewardship and safety of life and property.
- **Systems Engineering is both a technical and a management discipline**



Systems Engineering Challenges



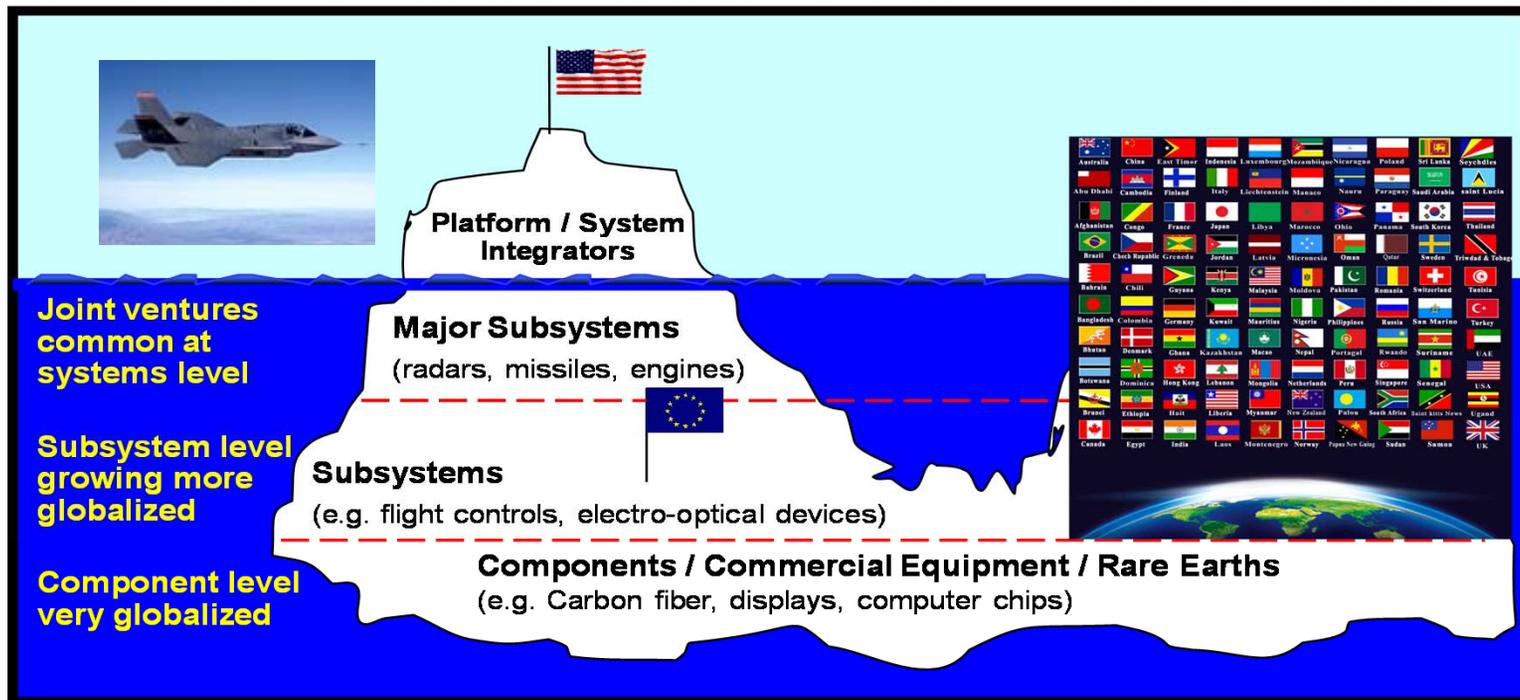
- **Start programs right with strong early SE**
- **Perform robust reliability and maintainability engineering**
- **Emphasize design for manufacturing**
- **Create the tools to support rapid capability delivery**
- **Reinvigorate Defense Standardization**
- **Expand the aperture of DoD engineering practice to address 21st century technical challenges**

All of these must be considered in how we address Counterfeit Prevention



Globalized Industrial Base

Industrial foundation becoming more integrated between the U.S., its allies, and global commercial markets



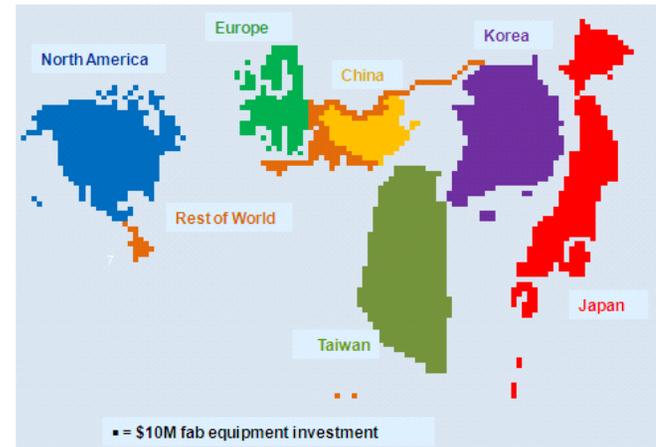
Growing dependence upon international commerce



Globalization of the Semiconductor Industry

- U.S. holds 48% semiconductor market share (sales)
- But . . . manufacturing capacity went from 25% (2005) to 14% (2009)
- Large portion of off-shore investment made by U.S. Corporations
- But . . . disproportionately low investment in U.S. capacity

If each region's size reflected its investment in new semiconductor equipment, Japan and Taiwan would be larger than North America, and Korea would be close.



U.S. Losing Share in New Semiconductor Manufacturing Capacity

% of World Semiconductor Fab Equipment Shipped to U.S.

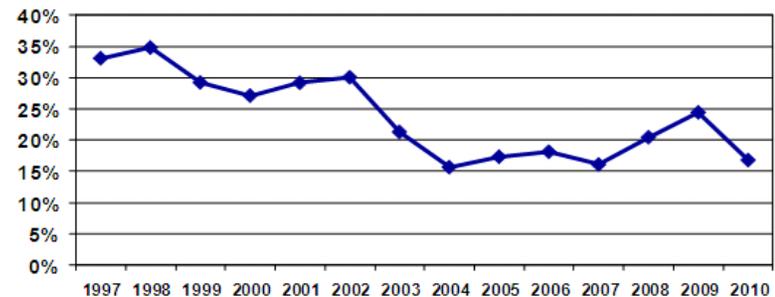
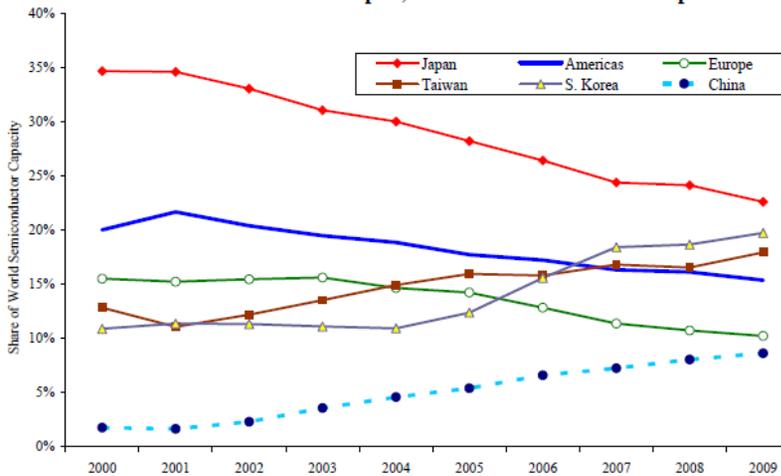


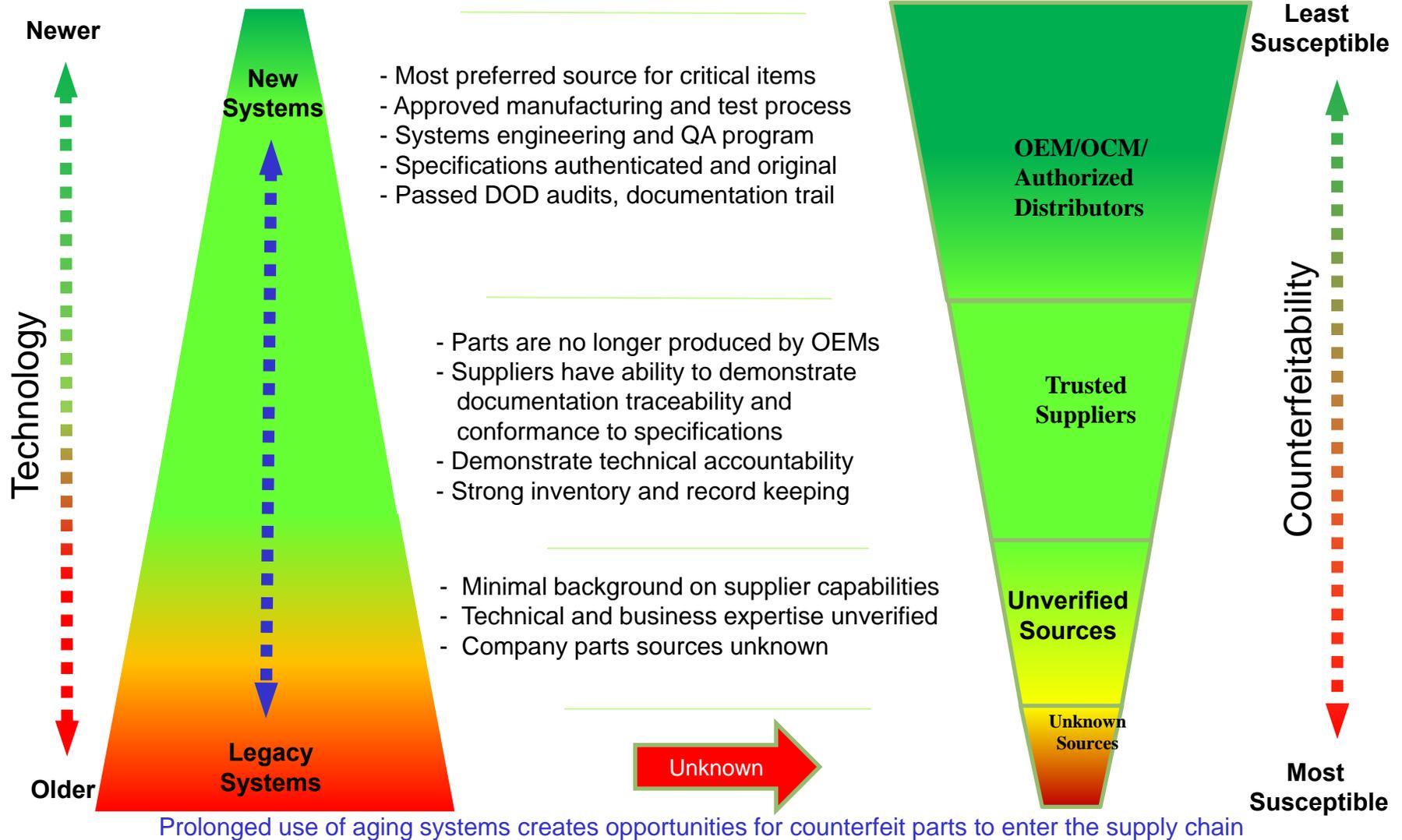
Chart 6: The Share of World Capacity Has Grown in Korea, Taiwan and China but Has Fallen in Japan, the United States and Europe



Source: SEMI, Industry Research & Statistics Department. Data beyond 2008:Q3 based on projections.



Profile of Counterfeit Risk





FY12 National Defense Authorization Act (NDAA) Section 818



Focus—Detection and Avoidance of Counterfeit Electronic Parts

Tenets:

- Directs DOD to *assess current anti-counterfeiting practices* and implement “risk-based” policies to address counterfeit
- Requires DOD and contractors whenever possible to buy electronic parts from the Original Component Manufacturer (OCM) or its authorized distributor(s)
- Directs DOD to *establish a “Trusted Supplier” program* to certify organizations that comply with industry standards on anti-counterfeiting
- Institutes cost recovery for counterfeit items
- *Re-affirms mandatory reporting (GIDEP) for incidents internal and external to DOD*
- Requires the Secretary of Homeland Security to establish a methodology for the enhanced inspection of electronic parts after consulting with the SECDEF as to the sources of counterfeit parts in the defense supply chain

Specific Actions:

- *Establish DOD-wide definition*
- *Issue anti-counterfeit mitigation guidance*
- *Issue remedial action guidance*
- *Create reporting process (GIDEP)*
- *Develop process to analyze and act on reports*
- *Incorporate in DFAR anti-counterfeit language*

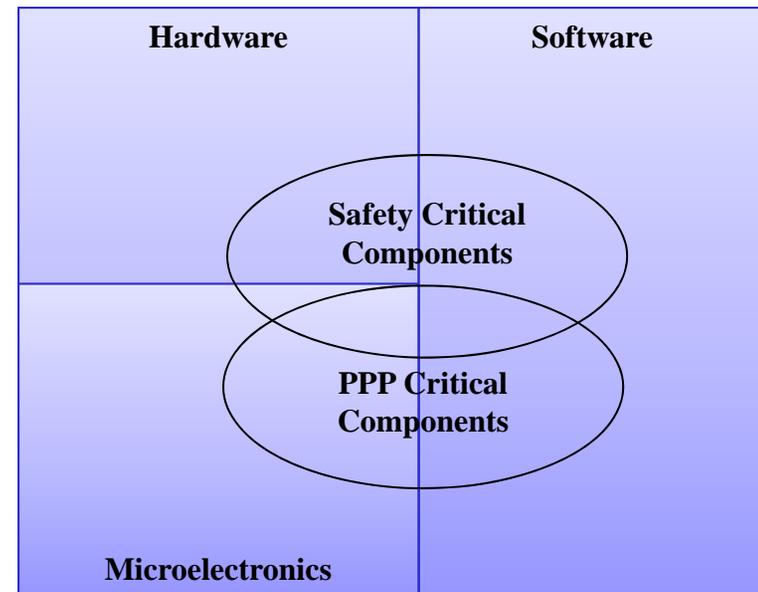




Counterfeit Problem Space



- **Counterfeits for Profit:**
 - Up-screened, re-marked, or re-used parts sold as new/authentic
 - Avoidable through OEM procurement; most should be detectable with sufficient inspection or test
- **Counterfeits for Malice:**
 - “Perfect” parts that also perform additional, unwanted functions
 - Designed to pass inspection
 - Must be combated with intelligence, Operational Security (OPSEC), and enhanced test & evaluation (T&E)



Counterfeits impact DoD safety, mission, and costs regardless of the motivation, but the techniques for combating them vary by motive



USD(AT&L) Memorandum: Overarching Counterfeit Prevention Guidance



 THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

MAR 16 2012

ACQUISITION, TECHNOLOGY AND LOGISTICS

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Overarching DoD Counterfeit Prevention Guidance

References: (a) PDUSD(AT&L) Memorandum, "Document Streamlining - Program Protection Plan (PPP)," July 18, 2011
(b) Defense Federal Acquisition Regulations Supplement, clause 252.246-7003, Notification of Potential Safety Issues, current edition

Counterfeit items are a serious threat to the safety and operational effectiveness of Department of Defense (DoD) systems. The Department is developing, with the participation of your staffs, policy and strategies designed to detect and prevent the introduction of counterfeit materiel. The policy and strategies will focus on those items that affect system performance or operation, the preservation of life, or safety of operating personnel. While we establish new DoD policy and procedures along with appropriate changes to the Defense Federal Acquisition Regulation Supplement (DFARS), this memorandum provides a broad framework and emphasizes the importance of taking action now to apply existing policy and procedures. This memorandum directs specific actions to prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain. For purposes of this memorandum, counterfeit materiel is defined as "an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." Additionally, a used item represented as a new item may also be subject to fraudulent representation procedures.

While the Department is concerned about counterfeits in all supply classes, particular focus is required for mission critical components, critical safety items, electronic parts, and load-bearing mechanical parts. DoD Components should immediately take action to decrease the probability of counterfeit items across the Department to include the following:

1. Ensure program managers are notified by their suppliers and contractors when critical items are not obtained from the original equipment manufacturer, original component manufacturer, or an authorized distributor, particularly where electronic parts are included. This requirement should apply to suppliers below the prime contract as well.
2. Require program managers to follow the Program Protection Plan Outline and Guidance (Reference (a)), which includes the requirement to evaluate counterfeit risk and implement countermeasures for mission critical components.
3. For other than mission-critical components, where the program or item manager has determined there is counterfeit risk that warrants action, the program manager or item manager must document risk mitigation within the program risk management plan or systems engineering plan.

8. Report suspected or confirmed counterfeit items discovered by DoD activities in GIDEP using the Product Quality Deficiency Reporting process as appropriate.

9. Investigate suspected counterfeit incidents discovered or reported, and report incidents confirmed as counterfeit to the appropriate criminal authorities. In the case of suspect counterfeits, the parts should be held until resolution of the potential non-conformance is complete. If items are confirmed to be counterfeit, they should not be returned to the actual or a potential supplier at any time prior to criminal authorities' release for disposition.

10. Develop and provide training to DoD personnel involved with the development, acquisition and procurement, supply, maintenance, and protection of weapon systems on proper measures to address counterfeiting.

Your support in this critical area will ensure the safety and mission performance of our warfighting systems. My point of contact is Mr. Gerry Brown, ODASD(SCI), at 571-372-5259.


Frank Kendall
Acting

2

- Addresses an area of critical concern while Department policy is in coordination
- Provides definition
- Emphasizes
 - Risk-based approach
 - Leverages Program Protection Plan and non-conforming processes
 - Directs use of contracting clauses and data elements to ensure traceability and reporting on critical items for contractors and subcontractors
 - Use of anti-counterfeiting standards
 - Disposal of counterfeit items
 - Training



Risk-based Counterfeit Prevention Strategy



- **Determine the risk posed if a part were identified as counterfeit**
 - Product Risk (the criticality of the product in which the part will be used)
 - Component Risk (the risk to the product that is associated with the failure of the part/component)
 - Supplier Risk (the risk incurred due to use of a selected manufacturer or distributor)
- **Broadly, gains can be made by evolving industry and supplier business practices for counterfeit avoidance and detection**
 - Raise the bar for industry and DoD counterfeit avoidance and detection
- **For mission-critical and safety-critical components, apply enhanced mitigations**
 - Trusted Defense Systems Strategy

Prevention ♦ Detection ♦ Remediation ♦ Reporting ♦ Restitution



Detection - Identification - Disposition



Counterfeit Part Detection

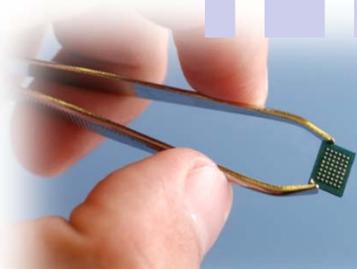
- Materiel control and traceability program
- Quality management systems
- Systemic test and verification processes

Identification

- Use product quality deficiency reporting processes
- Conduct engineering analysis and authenticity determination
- Report in GIDEP

Disposition

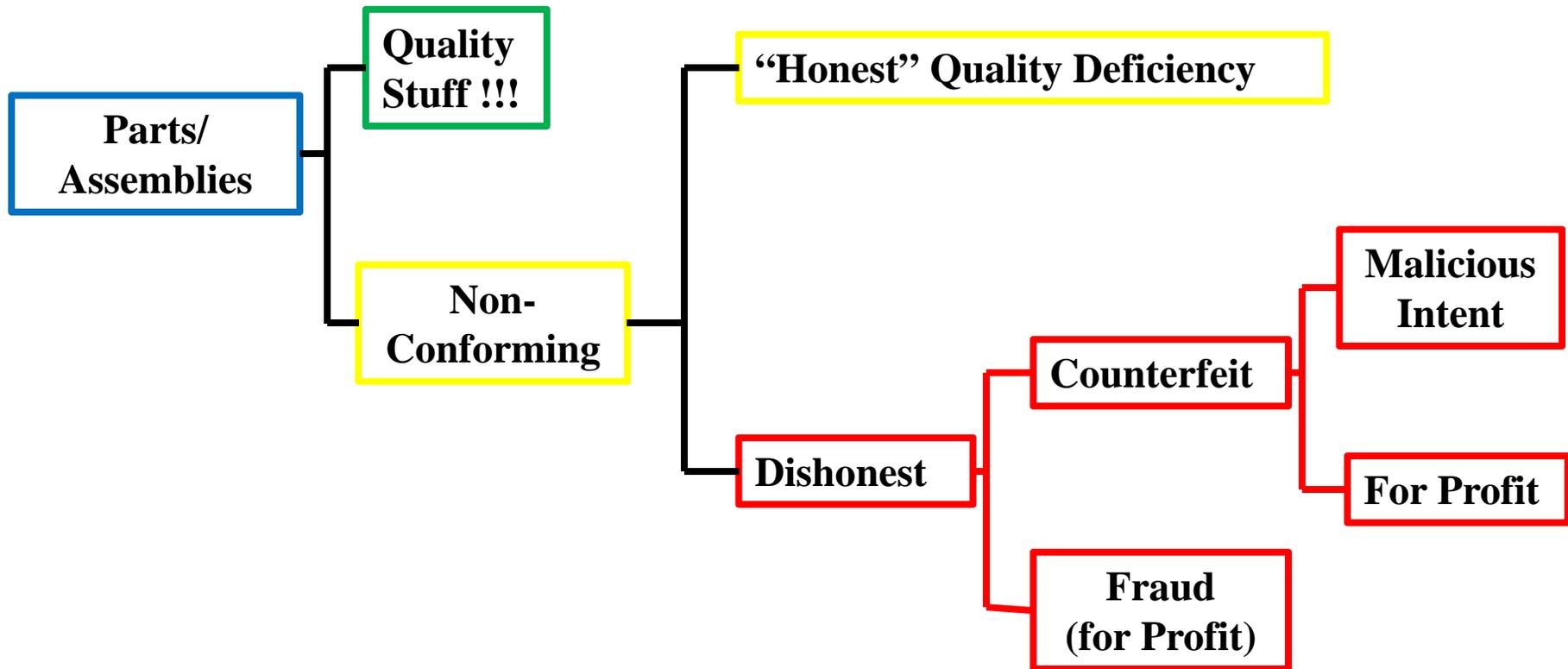
- Hold for law enforcement disposition
- Dispose according to federal logistics information system code guidance
- Execute suspension and debarment process as required



DoD Policy standardizing processes across supply chain



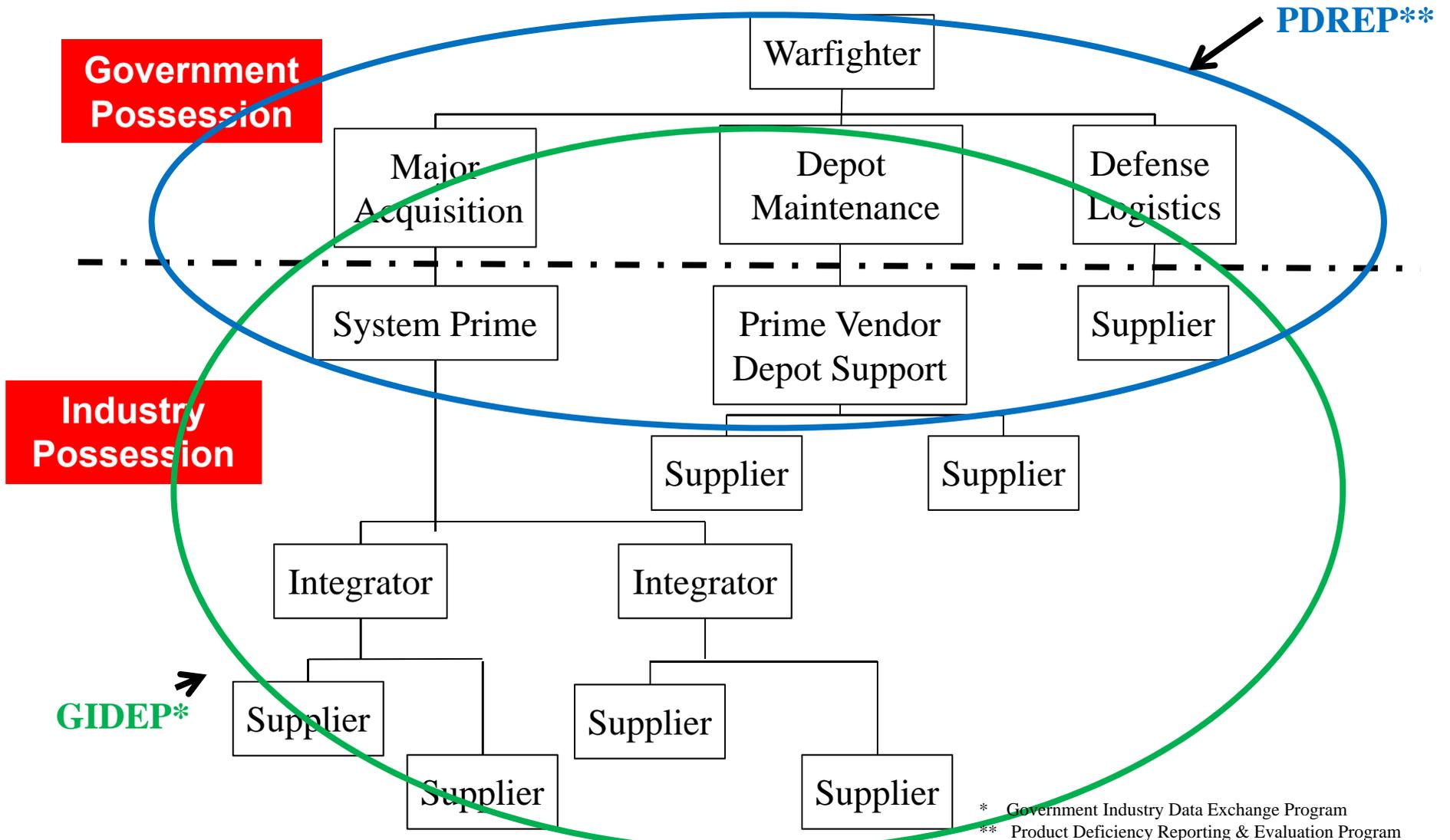
Non-Conformances





Gov't Acceptance – “The Dividing Line”

(that really does not matter)



* Government Industry Data Exchange Program
 ** Product Deficiency Reporting & Evaluation Program



Key Implementation Activities



Risk-based technical approach to lessen the impact of counterfeits

- **Acquisition Policy, Guidance, and Oversight**

- Defense Acquisition Guidebook (DAG)
- Systems Engineering Plan (SEP)

- **Program Protection Planning**

- Supply Chain Risk Management
- System Security Engineering

- **GIDEP information system; rules, regulations, reporting**

- **“Trustworthiness” of Suppliers**

- Defense Microelectronics Agency (DMEA) “Trusted” Supplier Program
- DLA QSL/D*
- Industry designated suppliers
- Inspection and Test philosophy

*Qualified Supplier List / Distributor



SEP: Systems Engineering Tables



Fiscal Year	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	22
Quarter	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4	1,2,3,4
Requirements																			
Acquisition Milest																			
Systems Engri																			
Logistics Eve																			
Major Contrac																			
Production																			
Training Syste																			
NEPA Schedu																			
Test Events																			
DITSCAP																			

Technical Schedule

Technical Review Criteria

Certification Requirements

Technical Performance Measures and Metrics

Design Considerations

Engineering Tools

Risks, Issues, and Opportunities

SVR Details Area	SVR Details
Chairperson	JAMS PM (or designee)
PMO Participants	LSE and IPT Leads
Anticipated Stakeholder Participant Organizations	Army PEO Missiles & Space, PEO Aviation, ATEC, AMRDEC and ASA(ALT), User community, AMCOM, T&E community (e.g., ATTC, ATEC, COMOPTEVFOR), Navy PMA 242, NAVAIR Competencies (4.0, 5.0).

Certification Effort	Acronym	Process Standard	P-BA IPT	Projected Completion Date	Actual Compliance Date
System Security Engineering – Information Assurance	(SSE - IA)	DODD 8500.1	SEIT	January 13, 2010	-



Name (Reference)	Cognizant PMO Org.	Certification	Document (hot link if available)	Contractual Req'ts (DID/CLIN)	Description/Comments
SE Tradeoff Analysis for Affordability	SEIT	N/A	CAIV Plan	In RFP CDRL	SEIT, in conjunction with Program IPT, oversees execution of CAIV Plan required by JAGM SOW to address traceable interdependent relationships between system performance, system reliability, Average Unit Production Cost (AUPC) and Life Cycle Cost (LCC). KPPs are not CAIV candidates. CAIV Plan directs specific CAIV trades

Application	Description
BORIS	Boeing Opportunity, Risk and Issue System database tool is a cooperative effort of Boeing Commercial Airplanes and Boeing Integrated Defense Systems.
ClearCase	Produced by Rational Software, Inc. ClearCase is a software configuration management system that keeps track of which versions of which files were
ClearQuest	
DOORS®	
MET	
Sherlock	
TecView	
Trade Studies Log	
VDATS	

Technical Risks	Mitigation Activities (Closure Dates)
R1. Failure to meet TOC reduction goals may cause budget exceedance	Continue current plan; expedite cuff/yoke redesign (Dec 2015)
R2. Main rotor cuff/yoke redesign not complete in time for test	Certification milestone plan developed and monitored by PM. (Jun 2011)
Technical Issues	
1. Production parts; spares	Continue focus on contractor's SCM and make parts (ongoing)
2. Structural Repair Manual late to need	Expedite approval of DL&T's (ongoing with NAVAIR)
Opportunities	
O1. Capture lessons learned; best practices; store in command library	Low investment; great benefit for program and NAVAIR



Counterfeit Prevention: Select DAG Chapter 4 Design Consideration Correlations



Design Consideration	Relationship
Reliability & Maintainability Engineering	Counterfeits that somehow get past receipt inspection and test can have radically different reliability and failure modes than the “honest” part.
Critical Safety Items	From an Anti-Counterfeiting Risk Based Approach, CSI are going to be more carefully scrutinized (inspected / tested) to ensure no counterfeits infiltrate supply.
ESOH	RoHS has driven increased number counterfeits where a lead-free microcircuit is sold as have tin-lead leads.
Corrosion Prevention and Control	Counterfeits, by their nature, may have falsely certified CPC. Additionally, if the counterfeit is a compound or component (e.g. gaskets; ground wires) intended to prevent or reduce corrosion, the effects may appear long before the predicted times and the impacts can be far worse.
Supportability	Increased failure rates can turn out to be due to counterfeits; unexplained failures can negatively impact supportability and might drive incorrect problem resolution behaviors.



Counterfeit Prevention: Select DAG Chapter 4 Design Consideration Correlations (cont.)

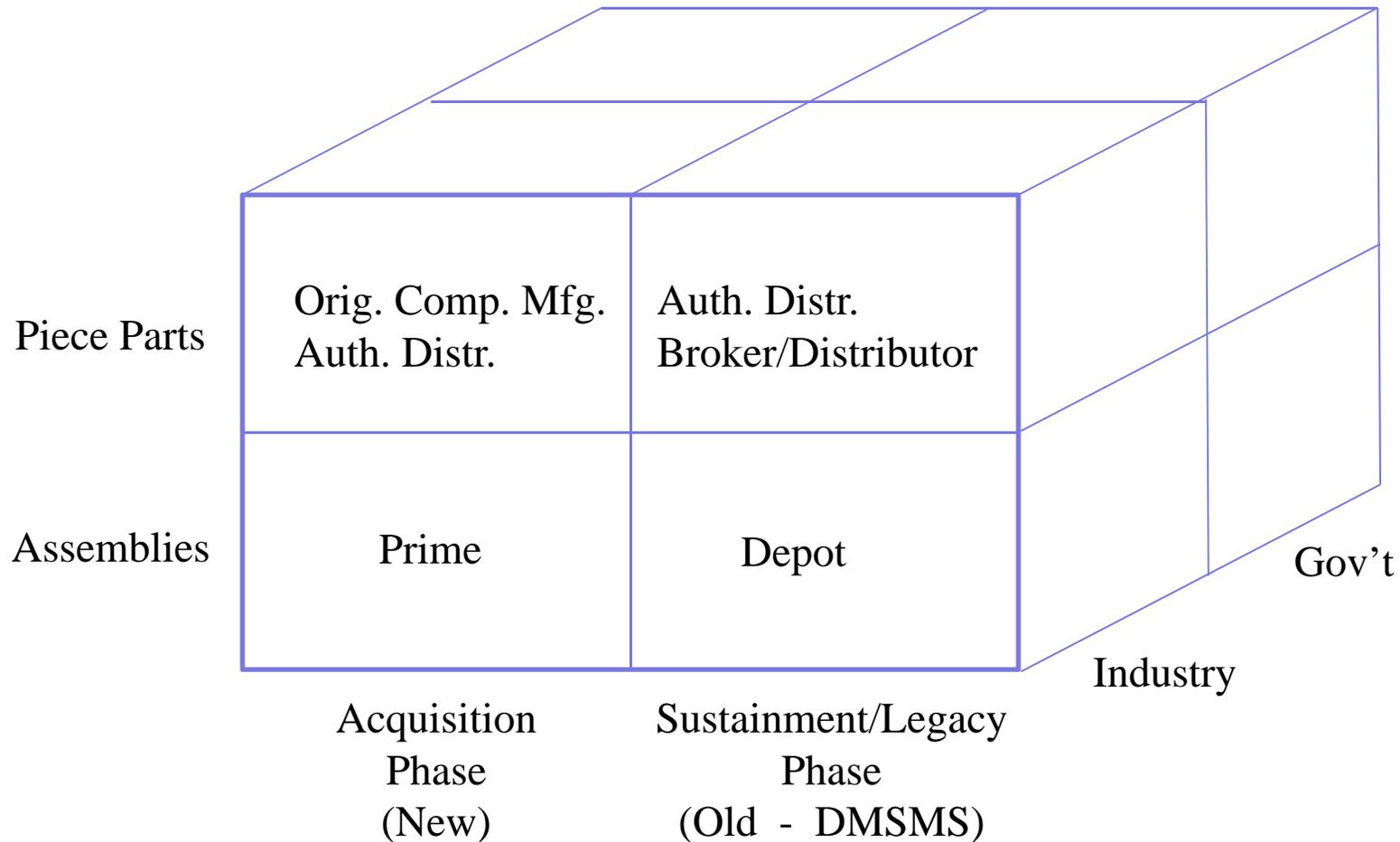


Design Consideration	Relationship
Commercial-Off-the-Shelf	The government and its industry agents will have considerably less visibility into the supply chains that create COTS products. An implication of this is counterfeit vulnerabilities as described in the other design consideration sections of this table.
DMSMS	As systems age and the trustworthy sources for the piece parts dry up, counterfeiters increasing take advantage of the situation by offering sources for hard-to-find-parts.
Disposal and Demilitarization	D&D is an excellent source for counterfeiters to obtain parts that can be turned into “used sold as new” parts (fraudulently certified as new).
Open Systems Architecture	OSA could provide a means to quickly certify a newer, more available part for use in weapon systems, thus reducing the impact of DMSMS. Conversely, it could also result in more part numbers (equivalents) being introduced into supply thus increasing the likelihood of counterfeit intrusion.



Trust In Supply

A business decision based on technical, industrial base, and supply chain factors





During Design



- **Engineers strive to optimize (among other things):**
 - Size, Weight, Power ...
 - Selected parts from approved lists to minimize logistics tail
 - Technologically advanced parts to meet the “requirement” for the new system
- **What do you do if every part may someday be suspect?**



Engineering Challenges

(brought on by counterfeits)



- **Different forms of counterfeit and fraudulent parts carry different reliability and performance curves.**
- **However, designing a system to be tolerant of counterfeits (if they get through the screening processes) is the biggest challenge engineers will face!**



GIDEP Reporting (Information Sharing Portal)



- **Most companies and agencies have some sort of “Quality Deficiency Reporting System”**
 - **GIDEP is a way of linking the knowledge in these systems together for the “collective good”**
-
- **Mandatory reporting of non-conformances (including suspected or confirmed counterfeits)**
 - **Coordination between GIDEP* and PDREP****
-
- **Modernize GIDEP system (entry; storage; retrieval)**
 - **Efficient correlation of specific issues to specific applications**

* Government-Industry Data Exchange Program

** Product Deficiency Reporting and Evaluation Program



How Industry Can Help



- **Tighten up your supply chain**
 - Establish benchmarks for good suppliers
 - Adopt / identify good non-government standards
- **Help us and each other by reporting Major and Critical Non-conformances, of which counterfeits is a subset**
- **“Design in” protection against counterfeits**



How Industry Can Help

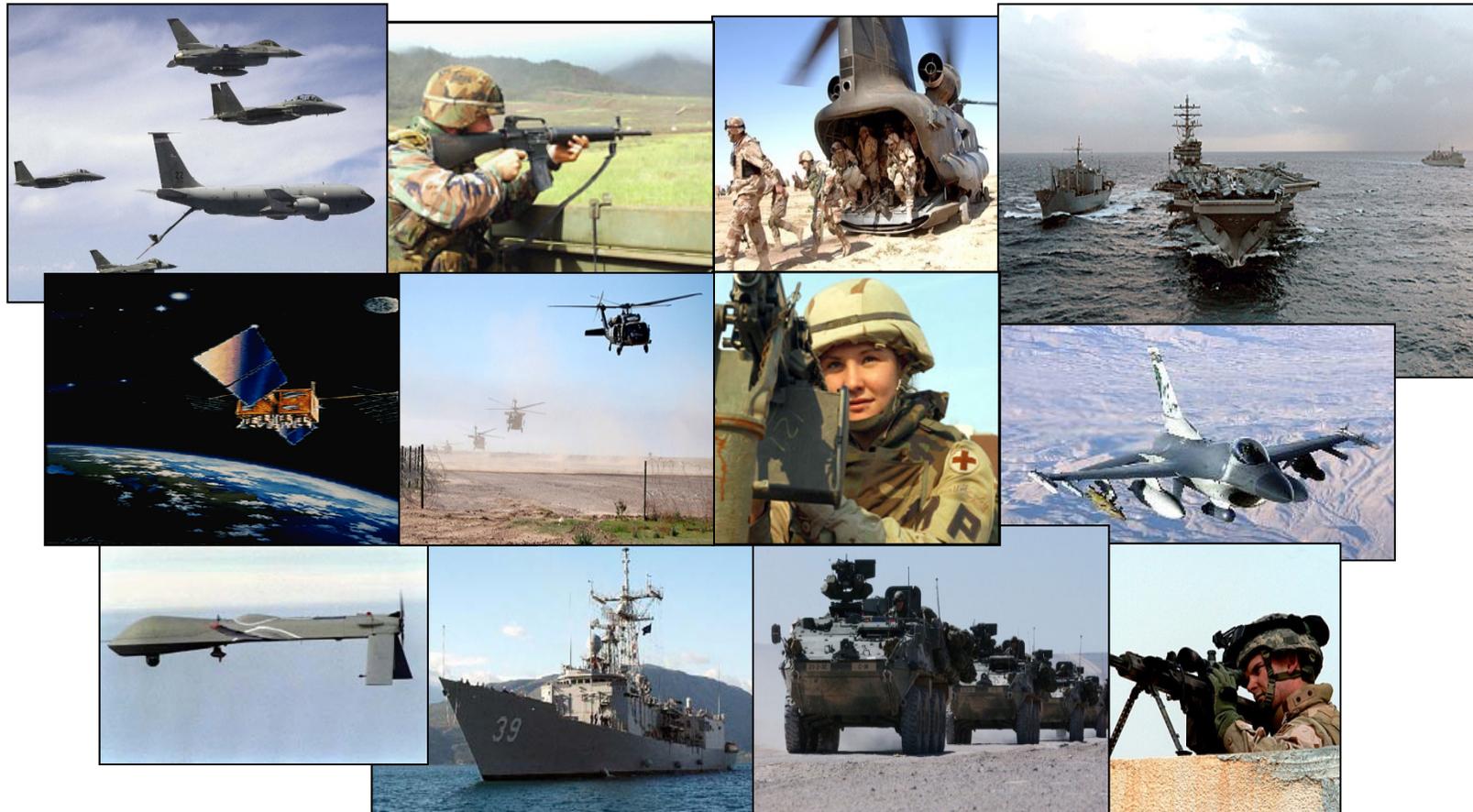
(from morning agenda)



- **Standards**
- **Identification**
- **Risk Assessment**
- **Avoidance Protocols**
- **Test Methodologies**
- **Compliance**



Systems Engineering: Critical to Program Success



Innovation, Speed, and Agility

<http://www.acq.osd.mil/se>