Space and Missile Systems Center

SMC Initiatives

21st Annual Components for Military & Space Electronics Conference & Exhibition

13 April 2017

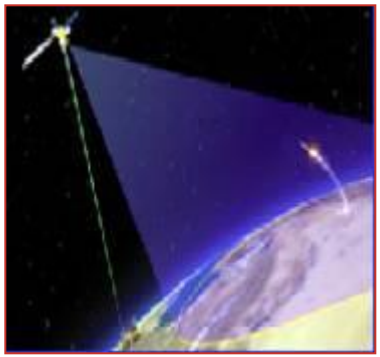
David Davis

SMC Chief Systems Engineer

SMC & PEO/Space Mission Overview

SPACE AND MISSILE SYSTEMS CENTER

WE DEVELOP, ACQUIRE, FIELD AND SUSTAIN SYSTEMS IN FOUR MAJOR MISSION AREAS



Space Superiority

Space Situation Awareness
- **SBSS**
- **Space Fence**

Defensive Counter Space
Offensive Counter Space

Space Support

Launch Systems
Spacelift Range
Sat Control & Network

Force Application

Conventional Missiles
Prompt Global Strike

Space Force Enhancement

Milstar/AEHF/EPS
DSCS/GBS/WGS
GPS
DSP/SBIRS
DMSP
NDS (Nuclear Detection)

Developing, Delivering, and Supporting Military Space and Missile Capabilities to Preserve Peace and Win Conflicts

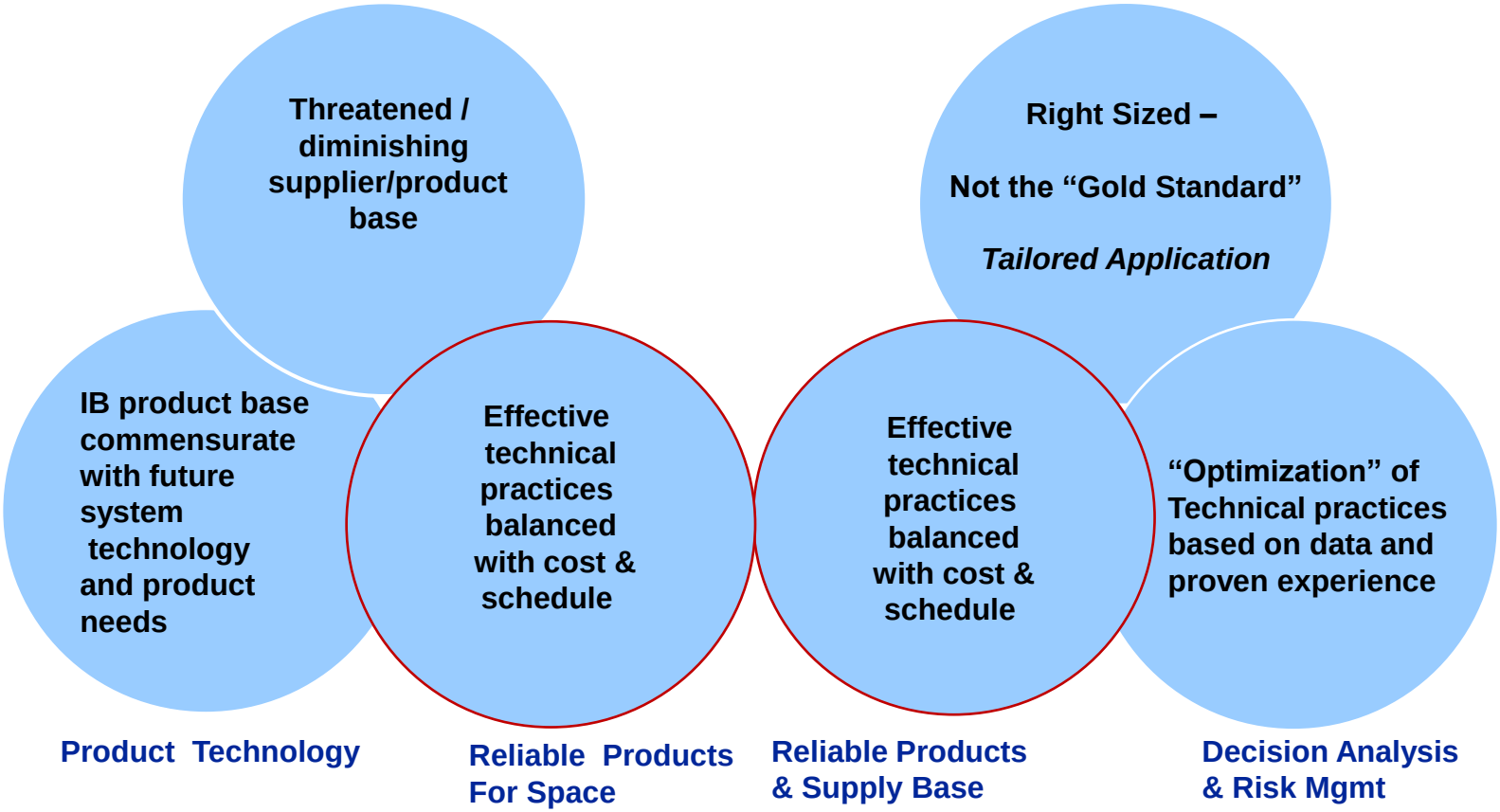
Space System Development

- Launch is a “one-strike-and-you’re-out” business
- Spacecraft must work by remote control for 15 years
  - Hostile environment
  - “Small” failures can cripple or end mission
  - No Beta Testing/LRIP and No On-Orbit Repair
  - Mandates Unique, High-Confidence Mission Assurance Culture

No “flight Testing” and No Service Calls in Space Mandates Unique, High-Confidence Mission Assurance Culture

Balancing the Needs for Space Acquisition

Space Industrial Base



Specs & Standards

Must Assure Critical Requirements and Industrial Supply Capability Necessary to Support Current and Future USG Space Programs

Example PM&P Activities/Issues

- **Looking at the AWARE items with impact to our programs :**
  - **3 programs or more**
    - **Bi-metallic Bonds IC construction without proper evaluation**
    - **Connector issues**
    - **Solid Ta caps with high ESR**
    - **Schottky Diode leakage issue**
  - **2 programs**
    - **Hermeticity failures leading to dendrites**
    - **Low tensile strength in Ti-6Al-4V**
    - **Cracks in steel wire stock**

Example PM&P Activities/Issues

- **Insufficient Testing**
  - **Screening methods/missing tests**
  - **Insufficient qualification testing**
- **Buyout of US manufacturers by foreign companies**
- **Use of commercial/automotive/plastic parts**
- **New technology insertion – Microcircuits, GaN, SiC**
- **DLA QML/QPL Spec/Stds Changes**
  - **EP study for Class Y (ceramic non-hermetic flip chip BGA/CGA devices) standard microcircuit drawings (SMD) boilerplate under MIL-PRF-38535**
  - **(EP) Study on Copper (Cu) wire bond test methodology for microcircuit, hybrid and semiconductor devices**
  - **Initial Draft of MIL-PRF-32535A (Capacitor, Chip, Fixed, Ceramic Dielectric (Temperature Stable and General Purpose), Extended Range, High Reliability and Standard Reliability, General Specification**
  - **Proposed changes in the x-ray criteria for seal voids as specified in MIL-STD-883 Test Method (TM) 2012**

Use of Automotive Parts

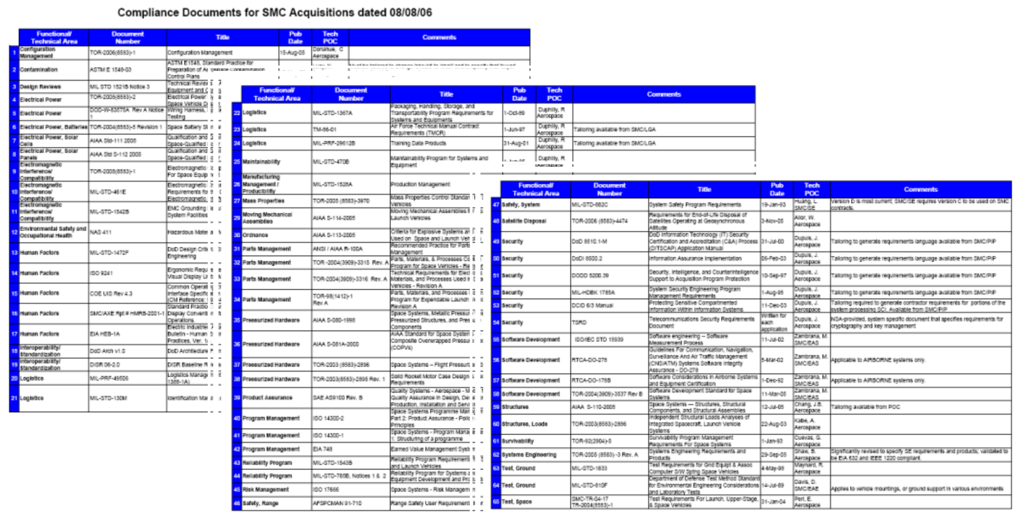
- **Objective:**
  - **Understand how suppliers implement their automotive product line in accordance with the AECQ100 requirements to include design, wafer fab, probe, assembly and test**
  - **Understand of qualification and process controls implementation to assure reliability and minimize lot to lot variations**

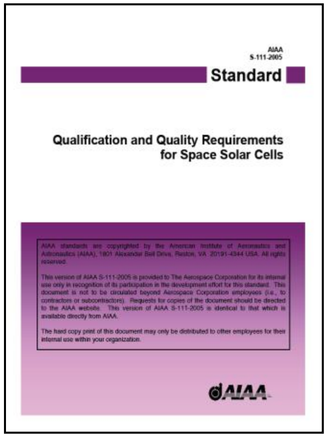
SMC Specifications & Standards Program

SMC Compliance Standards List

SPACE AND MISSILE SYSTEMS CENTER

- SMC Technical Baseline
  - 69 documents
- Includes all four space system segments
  - Military (MIL-STD)
  - International (ISO)
  - Industry (AIAA, IEEE, SAE, etc))
  - SMC Standards
- Reflects current best practices
- Updated periodically
- SMC Instruction 63-106, 31 July 15
- Applies to all new development, acquisition and sustainment contracts
- Contractual compliance through the supplier chain, as appropriate





Functional Areas of SMC Standards

Standard Practices

- Program/Subcontract Management
- ➢ Systems Engineering
- ➢ Architecture Development
- ➢ Design Reviews
- ➢ Configuration Management
- ➢ Quality Assurance
- Logistics
- ➢ Manufacturing /Production Management
- ➢ Parts Management (non-space)
- Parts Management (space)
- ➢ Risk Management
- System Safety
- ➢ Occupational Safety and Health
- Reliability/Availability

Subsystem/Component Standards

- ➢ Electrical Power, Batteries
- ➢ Electrical Power, Solar Cells/Panels
- Electromagnetic Interference & Control
- ➢ Environmental Engineering; Cleanliness
- ➢ Human Systems Integration
- Interoperability
- Maintainability
- ➢ Mass Properties
- ➢ Moving Mechanical Assemblies
- ➢ Ordnance
- ➢ Pressurized Systems & Components
- Information Assurance/Program Protection
- ➢ Software Development
- ➢ Structures
- Survivability
- Test, Space & Ground

➢ *Industry consensus standards developed or adopted for use on SMC contracts*

SMC/National Security Space PM&P Standards

- **SMC Standard SMC-S-009 (12 April 2013)**
  - **PARTS, MATERIALS, & PROCESSES CONTROL PROGRAM FOR SPACE VEHICLES**
  - **TOR-2006(8583)-2335 REV B, March 6, 2013, Parts, Materials, and Processes Control Program for Space Vehicles**
  - **Was Mil-Std 1546**
- **SMC Standard SMC-S-010 (12 April 2013)**
  - **TECHNICAL REQUIREMENTS FOR ELECTRONIC PARTS, MATERIALS, AND PROCESSES USED IN SPACE VEHICLES**
  - **TOR-2006(8583)-2336 REV B, March 6, 2013, entitled Technical Requirements for Electronic Parts, Materials, and Processes Control Program Used In Space Vehicles**
  - **Was Mil-Std 1547**
- **SMC Standard SMC-S-011 (31 July 2015)**
  - **PARTS, MATERIALS, AND PROCESSES CONTROL PROGRAM FOR EXPENDABLE LAUNCH VEHICLES**
  - **TR-RS- 2015-00011 , Parts, Materials and Processes Control Program for Expendable Launch Vehicles**
  - **Was part of Mil-Std 1546**

SMC Standards Program

- **SMC practices continue to evolve to commercial standards where/when feasible**
- **Transitioned numerous SMC space military standards (PA-19) to industry standards or SMC Standards**
  - **Active participation role in development/revision of industry standards, including co-chair roles**
- **Review standards on continuing basis to assess status and determine if any actions necessary**
  - **Revalidate; Revise; Cancel; Inactivate for new design (primarily for specifications)**
- **Cancellations completed - 2016**
  - **MIL-STD-1540, *Product Verification Requirements - Launch, Upper Stage, and SV***
    - **Includes reference to SMC-S-016 for future acquisitions**
  - **DOD-STD-1578, *Nickel-Cadmium Battery Usage Practices For SV***
  - **MIL-HDBK-1547, *Electronic Parts, Materials, and Processes for SV and LV***
  - **MIL-HDBK-83578, *Criteria for Explosive Systems and Devices use on SV***

SMC Standards Program

- **Cancellations in process – 2017**
  - MIL-STD-1576, *Electroexplosive Subsystem Safety Requirements for Space Systems*
    - Includes reference to AIAA-S-112
    - Project number SAFT-2017-001
  - MIL-STD-1541, *Electromagnetic Compatibility for Space Systems*
    - Includes reference to SMC-S-008 and AIAA-S-121
    - Project number EMCS-2016-004
  - MIL-HDBK-1811, *Mass Properties Control for SV*
    - Project number SPVT-2016-006
  - DOD-HDBK-343, *Design Construction, Testing for one-of-a-kind SV*
    - Project number SPVT-2016-005
  - MIL-HDBK-340, *Test Requirements for Launch, Upper Stage, and Baselines*
    - Project Number SVT-2016-007
- **Significant future actions required**
  - MIL-STD 1546, *Parts, Materials and Processes Control Program*
  - MIL-STD-1547, *Technical Criteria for, Parts Materials and Processes*
  - MIL-STD-1542, *Grounding, Facilities*

Maintenance of “over-age documents” in process IAW DSP procedures

ISO/IEC/ IEEE 15288, Systems and Software Engineering System Life Cycle Processes

- On behalf of DoD, SMC lead development of Systems Engineering and Technical Reviews & Audits Standards in partnership/collaboration with industry
  - Objective - develop and publish Systems Engineering and Technical Review and Audits Industry Standards
- Partnered with IEEE and leveraged ISO/IEC/ IEEE 15288, Systems and Software Engineering System Life Cycle Processes
  - Co-chaired with IEEE industry lead in vice-chair role
- SMC standards, SMC-S-001 and 021 primary source documents
  - 15288-1 published as addendum leveraging SE processes baselined in 15288 standard
  - 15288-2 published as “stand-alone” Technical Reviews & Audits standard tied to 15288 SE process

IEEE 15288 -1/-2 Standards Functionally Equivalent to SMC Standards

EMI/EMC

- SMC Standard SMC-S-008 currently used EMI/EMC standard
- AIAA S-121- 2009 Standard
  - Electromagnetic Compatibility Requirements for Space Equipment and Systems
  - Initiated under the sponsorship of the Air Force Space and Missile Systems Center (SMC) and under the auspices of the AIAA Electromagnetic Compatibility (EMC) Committee on Standards
    - Source document was “Electromagnetic Compatibility Requirements for Space Systems and Equipment," TOR 2005(8583)-1, 8 August 2005
  - MIL-STD-464 and MIL-STD-461 are the basis for electromagnetic effects requirements for military procurements for all platforms
- AIAA EMC CoS established to review/revise ANSI/AIAA S-121
- Intent is to replace SMC Standard SMC-S-008 with AIAA Standard

Draft Update In Team Review

SMC-S-017

Lithium-Ion Spacecraft Standard

- **Purpose: Update to current SMC lithium-ion spacecraft standard**
  - **Addresses lessons learned and best practices from implementing lithium ion battery technology over last 8 years**
  - **SMC-S-017 Standard**
    - **Was originally released in 2008 as a test standard**
    - **Battery centric (build, test, handling, storage, & on-orbit ops)**
      - **Very few cell level test requirements**
- **Draft SMC-S-017 standard**
  - **Adds Li-Ion battery general requirements**
    - **Cell & battery design, manufacturing, quality, and safety requirements consistent with current SMC practices and standards**
    - **Rules for cell and battery design requalification**
    - **Requirements for electronic assemblies within the battery**

Recently Completed 2nd Round of Govt/Ind Comments/Disposition

SMC Standard SMC-S-011

31 July 2015

Supersedes:
SMC-S-011 (2008)

SPACE AND MISSILE SYSTEMS CENTER STANDARD

PARTS, MATERIALS, AND PROCESSES CONTROL PROGRAM FOR LAUNCH VEHICLES

SMC 011 Parts Selection

- **Mission critical Component**
  - **System/circuit performing a function required to meet the mission objectives or flight safety requirements, regardless of redundancy or implementation scheme**
- **ELV Space PMP Baseline required for Category I**
  - **Category I - Mission Critical & Single String or Mission Critical & Single point Failure**
- **Program PMP Baseline allowable for Category II**
  - **Category II - Mission Critical and Redundant**
  - **Selection based on WCCA, Worst Case Derating, Redundancy, Mission reliability, Survivability**
    - **Prescribed part screening and class selection no longer required**
    - **Knowledge of manufacturer part control, technology, & failure modes**
  - **Baseline established by Contractor and approved by Parts, Materials, & Processes Control Authority (PMPCA)**
- **Non Mission Critical Applications**
  - **Do no harm analysis**

Survivability Standards

- **MIL-STD-3053-1**
  - **Satellite System Natural and Nuclear Environment Standard published Nov 2015. Compliance doc on GPS IV. Working to incorporate with SMC Chief Engineer's Compliance List.**
- **MIL-STD-3053-2**
  - **Satellite System Natural and Nuclear Protection Standard. 66% completed. Expected review cycle start date is Dec 2017.**
- **MIL-STD-3054**
  - **Endo-/Exo-Atmospheric Nuclear Environment Standard. Update underway to include Nuclear Disturbed Communication Environment and lower altitude detonations.**
- **Satellite System Protection Handbook**
  - **Expected publication in 2020**

Space System Test Resources and Infrastructure Study

Objective: Develop roadmap for mitigating shortfalls in resources and infrastructure that constrain the ability to conduct adequate testing for current and future space systems. Ref: OUSD AT&L Memo 6 Feb 2017

- **Identify current test resources**
- **Identify current and future test resource needs**
- **Identify and define gaps and shortfalls**
- **Develop resources and infrastructure gap mitigation roadmap**
- **Develop Congressional Report and Issue Paper(s)**

SMC Study POC: Dr Mark Johnson, The Aerospace Corporation

Tailoring
(Life Cycle)
Mission Assurance
(Big MA)

"Right Sizing" the
SMC Specifications
and
Standards Program

Proven and Disciplined Technical Practices At the Core of SMC's Mission Assurance Approach

- **Proven Practices:**
  - **Based on 5+ decades of space experiences and often painful lessons learned**
- **Mission Assurance: The culmination of all the things the contractor and government team does to achieve mission success**
  - **Engineering, business practices, incentives, contract type, tailored oversight**
- **SMC policy mandates use of S&Ss in SMCI 63-106**
  - **SMC works with program offices and contractors to tailor**
  - **Mission success, budget, cost, schedule, risk, affordability, and program performance carefully balanced**
  - **Tailoring not to delete or dilute a SS, but to implement the "intent" efficiently and economically**
  - **To provide confidence in achieving mission success and reduce program risk**
- **Published internal SMC "Mission Assurance Tailoring Guide"**
  - **SMC-G-007 (23 July 2013)**

S.2943 - National Defense Authorization Act for Fiscal Year 2017

- **SEC. 875. Use of commercial or non-Government standards in lieu of military specifications and standards.**
  - **(a) In general.—The Secretary of Defense shall ensure that the Department of Defense uses commercial or non-Government specifications and standards in lieu of military specifications and standards, including for procuring new systems, major modifications, upgrades to current systems, non-developmental and commercial items, and programs in all acquisition categories, unless no practical alternative exists to meet user needs. If it is not practicable to use a commercial or non-Government standard, a Government-unique specification may be used.**
  - **(b) Limited use of military specifications.**
- **(1) IN GENERAL.—Military specifications shall be used in procurements only to define an exact design solution when there is no acceptable commercial or non-Government standard or when the use of a commercial or non-Government standard is not cost effective.**
- **(2) WAIVER.—A waiver for the use of military specifications in accordance with paragraph (1) shall be approved by either the appropriate milestone decision authority, the appropriate service acquisition executive, or the Under Secretary of Defense for Acquisition, Technology, and Logistics.**
- **(c) Revision to DFARS.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall revise the Defense Federal Acquisition Regulation Supplement to encourage contractors to propose commercial or non-Government standards and industry-wide practices that meet the intent of the military specifications and standards.**
- **(d) Development of non-government standards.—The Under Secretary for Acquisition, Technology, and Logistics shall form partnerships with appropriate industry associations to develop commercial or non-Government standards for replacement of military specifications and standards where practicable.**

COUNTERFEIT PARTS

Parts, Materials & Processes Space Standards
SMC-STD 010/011

- Existing comprehensive PM&P management/technical program
  - Historically, effective at assuring quality parts, but “silent” on subject of counterfeit parts
- SMC sponsored the update/revision of two PMP Standards (Aerospace TORs) for Space and Launch Vehicles
  - Requires all PMP to be procured from the original qualified parts/materials equipment manufacture (OEM), or it’s franchised/authorized distributor
  - Requires all parts be delivered with a certificate of compliance to military specification or space-level-equivalent source control drawing
  - Requires contractor to approve subcontractor PMP
  - Requires contractor to establish date/batch number control and two-way tractability for PMP used in flight hardware
  - Requires contractor to perform Destructive Physical Analysis (DPA) consistent with program technical requirements and MIL-STD-1580

PMPCB / PMP Selection List

- **PMPCB**
  - **Requires establishment of a Parts, Materials and Processes Control Board (PMPCB) with the following responsibilities:**
    - **Review and approve all PMP**
    - **Establish and maintain all PMP lists**
    - **Review results of DPAs, Material Review Board (MRB) actions, and failure analysis.**
    - **Ensure laboratories and facilities used for screening and/or evaluation of PMP are adequate.**
    - **Establish and maintain a prohibited PMP list**
    - **Review all GIDEP, NASA, DOD, contractor, subcontractor and other agency PMP alerts, advisories, and reports for relevance to items used in the system.**
- **PMP Selection List**
  - **parts and materials are technically justified with approved and qualified sources of supply, approved procurement specifications, and defined application conditions**
- **Parts Procurement**
  - **All parts shall be procured from the part original equipment manufacturer (OEM) or its franchised, fully authorized distributor, and shall come with an OEM certificate of compliance.**

Additional Standards - Counterfeit

- **SAE AS-5553_**
  - Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
- **MIL-STD-3018; w/CHANGE 2; 2 June 2015**
  - DEPARTMENT OF DEFENSE STANDARD PRACTICE - PARTS MANAGEMENT
  - 3.4 Counterfeit part. A suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain. Parts which have been refinished, upscreened, or uprated and have been identified as such, are not considered counterfeit.
  - j. Counterfeit parts. The parts management plan shall address the detection, mitigation, and disposition of counterfeit parts. Electronic, electrical, and mechanical parts are to be addressed. AS5553 should be used as guidance for electronic parts.
- **SAE AS6500 (Manufacturing Management Program)**
  - SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
  - 5.4.1 Supply Chain and Material Management
    - d. Counterfeit Parts: The organization shall implement a counterfeit parts prevention program to prevent the acquisition and incorporation of counterfeit parts or parts embedded with malicious logic into factory and test equipment and delivered products. The program shall include procedures for prevention, detection, and reporting of counterfeit parts

Committee on Foreign Investment in the United States

(CFIUS)

Committee on Foreign Investment in the United States (CFIUS)

SPACE AND MISSILE SYSTEMS CENTER

- **The Committee on Foreign Investment in the United States (CFIUS) reviews foreign acquisitions, mergers and takeovers of U.S. businesses that raise national security issues.**
- **CFIUS, working by consensus, has the power to approve a transaction or send it to the President for his decision.**
- **CFIUS operates on statutory deadlines consisting of an initial 30-day review, a possible further 45-day investigation, and a possible Presidential decision lasting 15 days.**
- **CFIUS is chaired by the Department of Treasury (Treasury), and includes representatives from 15 other United States government departments, agencies and offices.**
- **While filing with CFIUS is generally voluntary, and the Committee reviews less than 10% of all inbound foreign transactions, it has the authority to compel a review of a transaction that is not filed voluntarily.**

SMC IB / CFIUS Assessment

- **Use of Product/technology on space systems**
  - **Is it a company that is critical to the space industrial base?**
    - Do they supply parts to SMC programs (Space, Ground, User Terminals)
    - Are SMC programs planning to use the supplier in the future
    - Do other NSS programs or NASA use this supplier
    - Do their products need to be Trusted though the DMEA process
    - Are they a single source or do other companies supply similar or identical parts at the same level of trust
    - How long would it take to reconstitute the capability
  - **Is the company's technology critical to SMC?**
    - Does this company possess Intellectual Property (IP) that is critical to SMC and other space providers.
    - Has the government invested in the company to help them create the IP needed for NSS programs
    - Does this IP extend beyond the space community; Does it effect other DOD areas
    - Is the company ITAR compliant
    - Does the IP need to be ITAR protected from the foreign buyer
    - Is their customer's IP (designs, masks, ...) potentially vulnerable, with the new company construct
    - Do other companies/sources have equivalent IP for use on SMC programs
      - if so, do they have sufficient protections in place to protect their customer's IP

Long-Term Strategy for DoD Trusted Foundry Needs

Cybersecurity / Supply Chain Risk Management (SCRM)

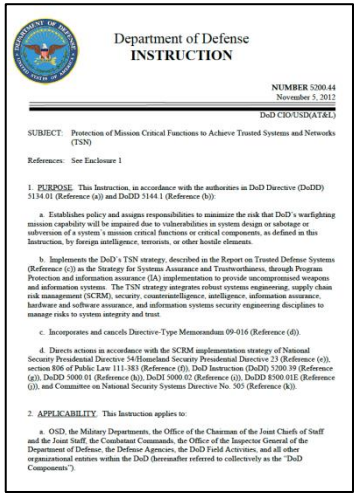
Kristen J. Baldwin
Principal Deputy
Office of the Deputy Assistant Secretary of Defense for Systems Engineering, OUSD(AT&L)

Trusted/Cyber/SCRM Policy

Trusted Systems and Networks (TSN)

- **DoDI 5200.44, August 25, 2016**
  Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

Strategy for Systems Assurance and Trustworthiness, through Program Protection and cybersecurity implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, cybersecurity, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust."



Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012
DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

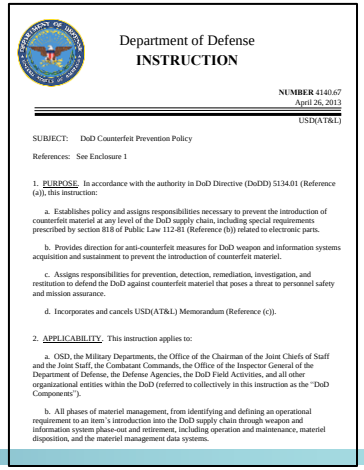
2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

Counterfeit Prevention

- **DoDI 4140.67, April 26, 2013**
  DoD Counterfeit Prevention Policy

"Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DoD supply chain"



Department of Defense
INSTRUCTION

NUMBER 4140.67
April 26, 2013
USD(AT&L)

SUBJECT: DoD Counterfeit Prevention Policy

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5134.01 (Reference (a)), this instruction:

a. Establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DoD supply chain, including special requirements prescribed by section 818 of Public Law 112-81 (Reference (b)) related to electronic parts.

b. Provides direction for anti-counterfeit measures for DoD weapon and information systems acquisition and sustainment to prevent the introduction of counterfeit materiel.

c. Assigns responsibilities for prevention, detection, remediation, investigation, and restitution to defend the DoD against counterfeit materiel that poses a threat to personnel safety and mission assurance.

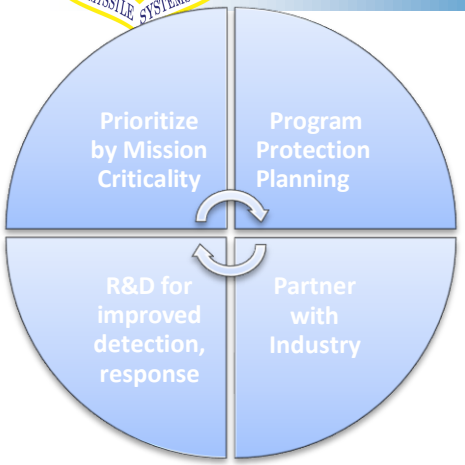
d. Incorporates and cancels USD(AT&L) Memorandum (Reference (c)).

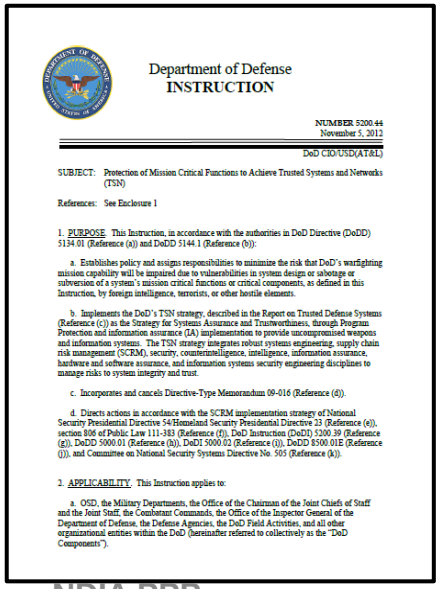
2. APPLICABILITY. This instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

b. All phases of materiel management, from identifying and defining an operational requirement to an item's introduction into the DoD supply chain through weapon and information system phase-out and retirement, including operation and maintenance, materiel disposition, and the materiel management data systems.

DoD Trusted Systems and Networks Strategy and Policy





Department of Defense
INSTRUCTION

NUMBER 5200.44
November 5, 2012

DoD CIO/USD(AT&L)

SUBJECT: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

Promulgated in DoDI 5200.44, requiring:

- **Risk management of mission-critical function and component compromise throughout lifecycle of key systems by utilizing**
  - **Criticality Analysis** as the systems engineering process for risk identification
  - **Countermeasures**, including supply chain risk management, software and hardware assurance, secure design patterns
  - **Testing and Evaluation**, to detect HW/SW vulnerabilities
  - **Intelligence analysis** to supplier acquisition strategies
- **DoD-unique application-specific integrated circuits (ASICs) must be procured from trusted certified suppliers**
- **Plans and mitigations documented in program protection and information assurance activities**

Distribution Statement A – Approved for public release by DOPSR on 5/14/14; SR# 14-S-1577 applies. Distribution is unlimited

Spectrum of Supply Chain Risks

Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

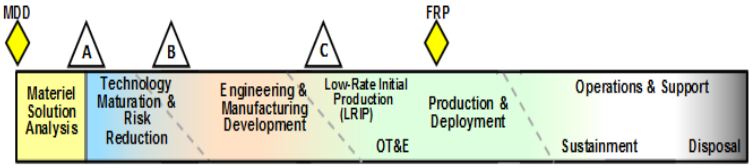
DoD Program Protection focuses on risks posed by malicious actors

Ensuring Confidence in Defense Systems

SPACE AND MISSILE SYSTEMS CENTER

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information
    - Disrupt or degrade system performance
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - All systems, networks and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled defense information resident on, or transiting supply chain networks
  - Loss or sale of US capability that provides a technological advantage
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact
  - Loss of US capability that provides a technological advantage

Access points are throughout the acquisition life cycle…

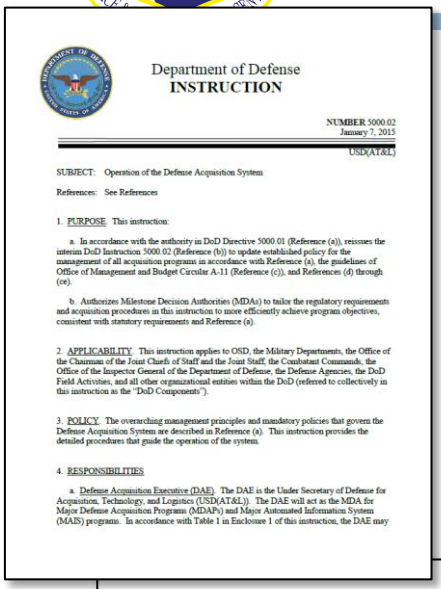


…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Program Protection Planning Policy

SPACE AND MISSILE SYSTEMS CENTER



Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (ee).

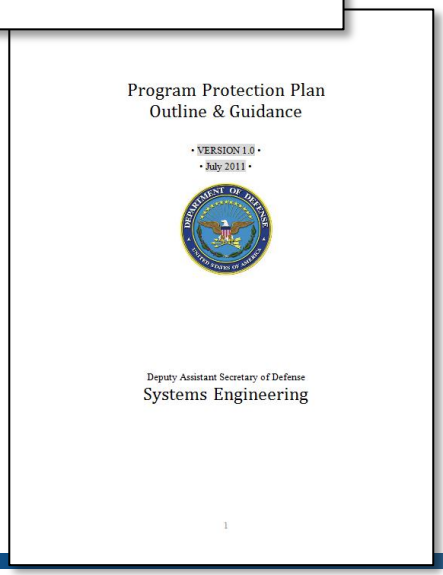
b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES

a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may



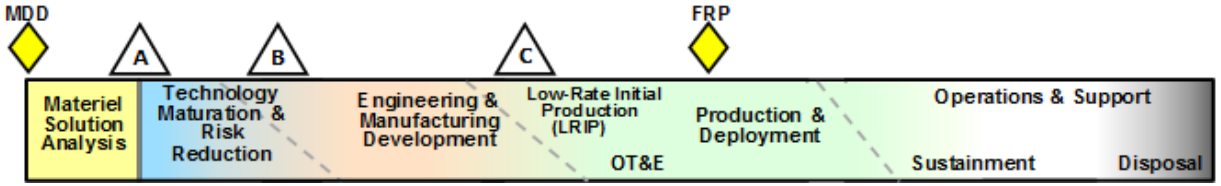
Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

1

- **System Security Engineering is accomplished in the DoD through program protection planning (PPP)**
- **DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a Program Protection Plan to manage the security risks to critical program information, mission-critical functions and information**
- **Program managers will describe in their PPP:**
  - **Critical Program Information, mission-critical functions and critical components, and information security threats and vulnerabilities**
  - **Plans to apply countermeasures to mitigate associated risks:**
    - **Supply Chain Risk Management**
    - **Hardware and software assurance**
  - **Plans for exportability and potential foreign involvement**
  - **The Cybersecurity Strategy and Anti-Tamper plan are included**



Long Term Trusted Foundry Strategy

Supports activities to ensure critical and sensitive integrated circuits are available to meet DoD needs

Program goals:

- **Protect microelectronic designs and intellectual property (IP) from espionage and manipulation**
- **Advance DoD hardware analysis capability and commercial design standards, e.g., physical, functional, and design verification and validation**
- **Mature and transition new microelectronics trust model that leverages commercial state-of-the-art (SOTA) capabilities and ensures future access**

Technical challenges:

- **Develop alternate trusted photomask capability to preserve long-term trusted access and protection of IP**
- **Scale/enhance the government's ability to detect security flaws in integrated circuits**
- **Leverage academic and industry research for assuring trust from any supplier**

Program partners:

- **DoD science & technology (S&T), acquisition communities, academia, industry**

Provides technical solutions that can be leveraged by government and industry to enable microelectronics trust

Long-Term Strategy Investment Summary

Compete/award alternate trusted photomask source for select IBM-unique technology needs and consolidate DoD Trusted Foundry Program management at the Defense Microelectronics Activity (DMEA)

- **Secure trusted photomasks required for leading-edge designs when using foundries other than GF Trusted Foundry**
- **Transfer National Security Agency (NSA) TAPO roles and responsibilities to the DMEA**
- **Engage and support DoD programs to determine advanced procurement strategies**

Improve DoD microelectronics evaluation capabilities (destructive/non-destructive) and develop commercial standards to make trusted parts a competitive advantage

- **Demand to analyze commercial parts will increase. DoD labs require tools/techniques to analyze leading-edge technologies and to improve throughput required for analysis**
- **Destructive and non-destructive equipment, analysis tools, imaging software and highly skilled tradecraft will be improved**
- **Engage vendors to improve their device and IP security; acquire government access to specific proprietary designs, software, development and quality assurance processes and test procedures**
- **Develop commercial standards that minimize security flaws and facilitate verification**

S&T program to develop and demonstrate alternative approach to the Trusted Foundry model

- **S&T program of work to advance technologies and implement an alternative to the trusted foundry model**
- **Technologies include: design for trust techniques; IP partitioning and concealment; split manufacturing; cost-effective low-volume manufacturing; tagging technologies to track chain of custody; advanced imaging and forensics to evaluate dense components**

Long-Term Strategy Time Line

Trusted Foundry Projects

SPACE AND MISSILE SYSTEMS CENTER

Alternate Source for Trusted Photomasks

Preparation activities	Capability Development	Deploy new capabilities

Verification and Validation (V&V) Capabilities and Standards for Trust

Preparation activities	Improve capabilities and capacity, and provide support to program needs, for analysis of microelectronics trust
	Identify and develop standards, practices, and partnerships to improve availability of trust from commercial providers

Advanced Technology and Alternative Techniques for Microelectronics Hardware Trust

Preparation activities	Capability development and demonstration	Deploy new capabilities and approaches

Related activities supporting the long-term strategy:

Programs fund and execute LTBs*

- During this period, acquisition programs fund and execute LTBs using the Trusted Foundry
- Work with GF to preserve Trusted Foundry

DPA Title III Project for photomask facility upgrade at Trusted Supplier

Upgrade

- Provides upgrade to mask tooling and secure processing at Trusted Supplier's facility required for the alternate source

DoD Trusted Foundry Program Consolidation

Transition

- Consolidates NSA TAPO's role and responsibilities for DoD Trusted Foundry Program at DMEA

2015 2016 2017 2018 2019 2020 2021 2020 2023 2024

Space Industrial Base Working Group (SIBWG)

Title-III Trusted FPGA Project

Dave Davis, USAF
DPA Title-III Trusted FPGA Technical Lead
SMC Chief Systems Engineer (SMC/EN)

Gabe Mounce, USAF
Space Electronics Tech Program
Air Force Research Lab

Project Mission

“This project seeks to improve the security posture and reduce the risk associated with FPGA technology by addressing security concerns in the design, development, fabrication and supply lifecycle of FPGA devices.”

Trust Definition

Concerning this effort "Trust" is defined as a device that will operate as intentionally designed and not contain any malicious hardware and/or software that will compromise the intended application

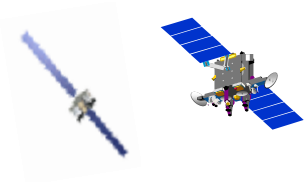
Space and Missile Systems Center

Future NSS Space Programs

SMC Next Generation Programs

- **The Changing Space Landscape**
  - **Evolving and greater threats (contested, congested, competitive)**
  - **Higher dependency on space systems (both military and commercial)**
  - **Funding constraints (DoD budgets flat at best)**

- **Challenges to the Current Architecture**
  - **Inflexible constellations (hard to maintain and replenish)**
  - **Lack of Resilience**
  - **Technology Stagnation and lack of competitive forces**
  - **Shrinking Industrial Base**
  - **Rising Cost**



- **Current architecture does not adequately address these new challenges**

- **AFSPC developing future resilient/affordable architectures and near-term investment strategies**

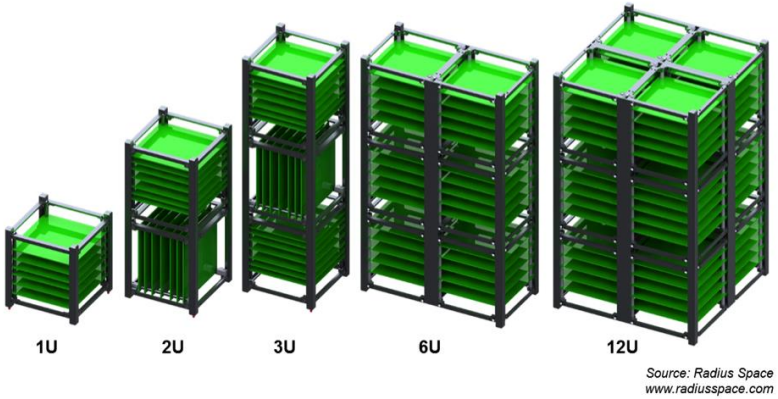
Compelling need for alternative space architecture options

SMC Architecture Studies On-going – Next "Programs of Record" TBD

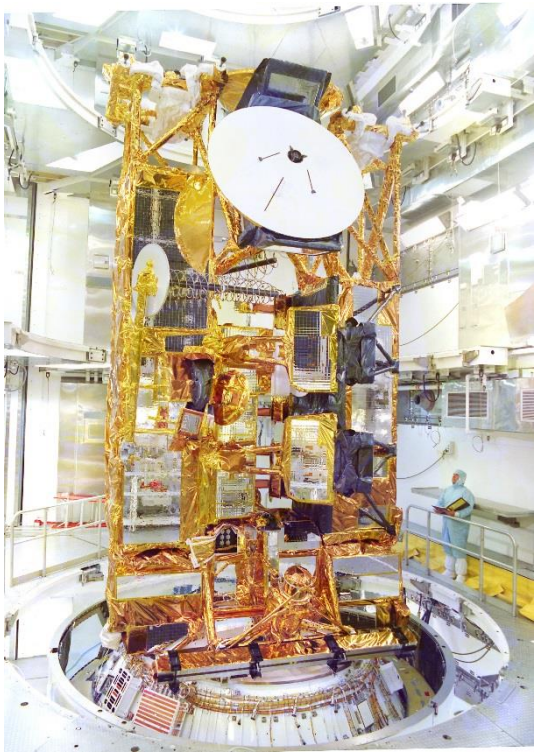
Space Enterprise Vision - Basis of Future Space Systems Architectures

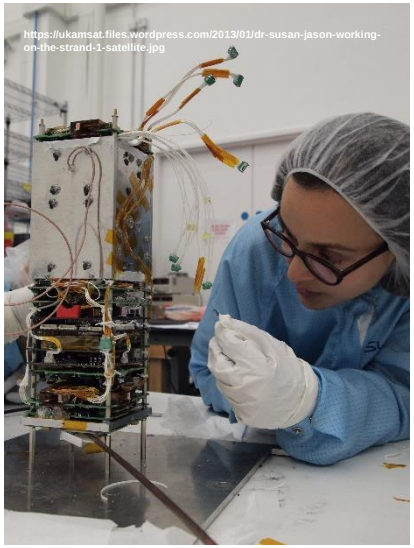
- In 2015, AFSPC/CC Gen Hyten called for a new Space Vision that he still endorses as STRATCOM/CC
  - Gen Raymond, the new AFSPC/CC is also a strong advocate of the new Space Vision
- November 2016, CNN War In Space TV special, highlighted threats that are real today!
- In the past, DoD requirements resulted in designs that focused on long-term functionality and long (15 year) operational lives
  - Time to think about 5 year designs, lower complexity, and block builds
  - Allows us to keep pace with rapidly evolving threats to on-ramp newest improvements, lower launch cost, etc.
- Acquisition processes and development cycles too slow to respond to dynamic threats
  - Pursuing prototypes, seeking new contractual vehicle's, RCOs, ORSs, OTAs, BAAs, Universities etc., adaptation of commercial methods and innovations where possible
  - Disaggregation of strategic and tactical, proliferation, small sats, hosted payloads, etc
- Need to seriously pursue enterprise solutions and how multiple systems, integrated together, could be more resilient than individual systems going it alone
  - Must learn to more synergistically operate as an enterprise, not just as independent platforms

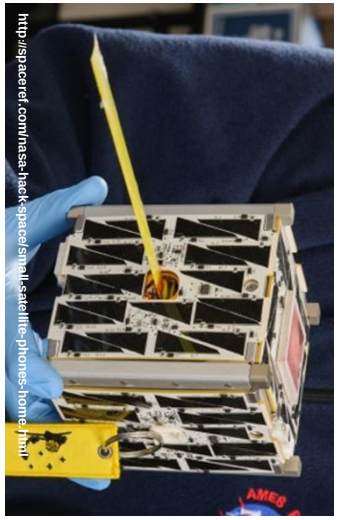
Nano, Cube, Small…….Sats



Source: Radius Space
www.radiusspace.com







Testing Foundation/Principles

- **High reliability required of all launch and space equipment achieved by the designs, design margins, and by the manufacturing process controls imposed at each and every level of assembly**
  - **Design & design margins assure equipment capable of performing in launch and space environment.**
  - **Manufacturing process controls intended to assure a quality product is manufactured that meets design requirements - any changes required made based on a known baseline**
- **Qualification tests conducted to demonstrate that the design, manufacturing process, and acceptance program produce mission items that meet specification requirements**
  - **In addition, the qualification tests will validate the planned acceptance program including test techniques, procedures, equipment, instrumentation, and software.**
- **Qualification Hardware subjected to qual testing will be produced from the same drawings, using the same materials, tooling, manufacturing process, and level of personnel competency as used for flight hardware.**
- **Acceptance tests conducted to demonstrate the acceptability of each deliverable item**
  - **Tests demonstrate conformance to specification requirements and provide quality-control assurance against workmanship or material deficiencies.**
  - **Acceptance testing is intended to stress screen items to precipitate incipient failures due to latent defects in parts, materials, and workmanship.**

Testing Foundation/Principles

- **Rationale for Retest**
  - **Retest is the repeat of previously conducted tests due to a redesign, a change in a manufacturing process, a test discrepancy, an increase in flight environments, or rework of items previously tested**
    - **Minor changes in design, manufacturing processes, flight environments, or rework can have a significant effect on the reliability of flight hardware**
  - **Requalification After Redesign – verification that design modifications have not introduced unpredictable failure mechanisms in the hardware**
  - **Requalification After Process Change - assurance that new process has not had a deleterious effect on the capability or reliability of the hardware**
    - **Assure that unpredictable changes have not been induced in manufactured hardware**
- **Piece Part Production Lot**
  - **A production lot of parts refers to a group of parts of a single part type; defined by a single design and part number; produced in a single production run by means of the same production processes, the same tools and machinery, same raw material, and the same manufacturing and quality controls.**
  - **All parts in the same lot have the same lot date code, batch number, or equivalent identification.**

Foundational Principles Will Need To Be Adapted For Future Systems

Summary

- **Continued focus on making space systems more affordable**
  - **Right Sizing Mission Assurance**
  - **Update standards as necessary to maintain currency with industry practices**
- **Support evolving new architectures - SEV**
  - **Affordable and resilient**
  - **Establish appropriate acquisition and mission assurance practices consistent with the program resiliency strategy/risk**
  - **Acquisition processes and development cycles which are more responsive to dynamic threats**
- **Establish practices and mitigation expectations for System Security Engineering / Trust/ SCRM**
  - **Trust, anti-tamper, cybersecurity, supply chain, software assurance, etc**

Thank You