21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

Hardware Assurance (HwA) Through the Lifecycle

Raymond C. Shanahan

Office of the Under Secretary of Defense for
Research and Engineering

October 24, 2018

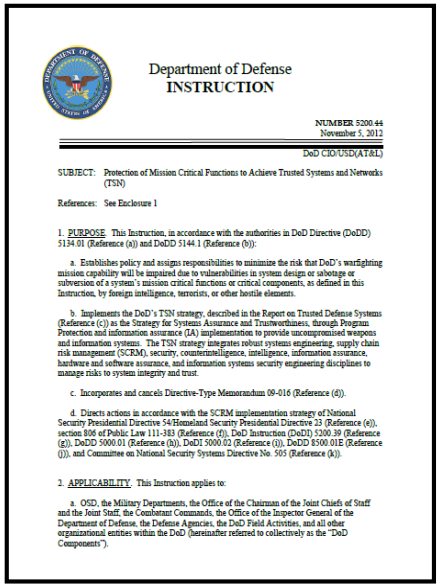
Key HwA Terminology and Policy

Key Terminology

Understanding the terms:

- **Hardware Assurance (HwA) (Defense Acquisition Guidebook (DAG) Chapter 9)**
  - The level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.
- **Criticality analysis (DoD Instruction (DoDI) 5200.44)**
  - An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s).
- **Critical components (CCs) (DoDI 5200.44)**
  - A component which is or contains [information and communication technology] ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.

HwA in DoD Trusted Systems and Networks (TSN) 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:

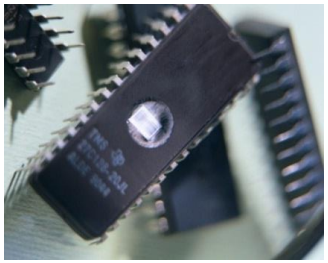
a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD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

Promulgated in DoDI 5200.44, requiring:

- **Risk management of mission-critical function and CC compromise throughout lifecycle of key systems by utilizing**
  - **Criticality Analysis** as the systems engineering process for CC and related risk identification
  - **Countermeasures**, including supply chain risk management, software and ***hardware assurance***, secure design patterns
  - **Testing and Evaluation**, to detect hardware and software 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 cybersecurity activities**

Applicability of HwA

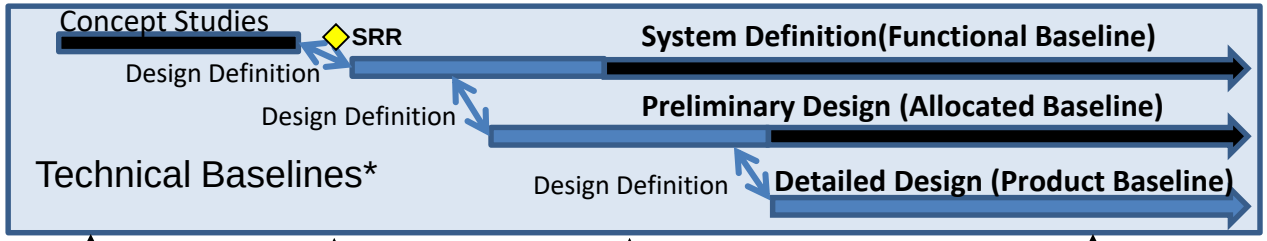
- **Applicable systems include:**
  - "(1) National security systems as defined in section 3552 of title 44, United States Code. …
  - (2) Any DoD system with a high impact level for any of the three security objectives (confidentiality, integrity, and availability) in accordance with the system categorization procedures of DoDI 8500.01; or
  - (3) Other DoD information systems that the DoD Component's acquisition executive or chief information officer, or designee, determines are critical to the direct fulfillment of military or intelligence missions …" (DoDI 5200.44)
- **Examples of microelectronics that may be critical and require HwA protections include vulnerable custom ASICs, programmable logic devices (e.g., Field Programmable Gate Arrays [FPGAs]), microprocessors, Application Specific Standard Products, and memories**



How do we identify them and mitigate the risk?

HwA within Systems Security Engineering (SSE)

SSE Activity Overview



- Protections are identified and integrated into technical baselines
- Analyses are iteratively informed by and informing the design
- Results are documented in the Program Protection Plan (PPP)

Program and System Analyses

Criticality Analysis
- Determine critical functions and components based on critical mission threads
- Identify key suppliers

CPI Analysis
- Identify capability elements providing a U.S. technological advantage
- Conduct horizontal analysis

Information Analysis
- Properly apply classification and marking procedures
- Implement required info protections

Threat and Vulnerability Assessments

Identify threats and vulnerabilities related to:
- Mission-critical functions/components
- Critical Program Information
- Key info about the program and system (emphasis on technical information)

SSE Decision Analysis

Assess SSE risks based on program/system analyses and identified threats/vulnerabilities

Determine candidate protections to address vulnerabilities. Utilize protections from across SSE specialties (e.g., anti-tamper (AT), HwA, cybersecurity) and security specialties (e.g., physical security, operations security)

Conduct engineering risk/cost trade-off analyses

Establish protection measures
- System security requirements
- Identify acquisition mitigations
- Further analyses necessary

Contractor

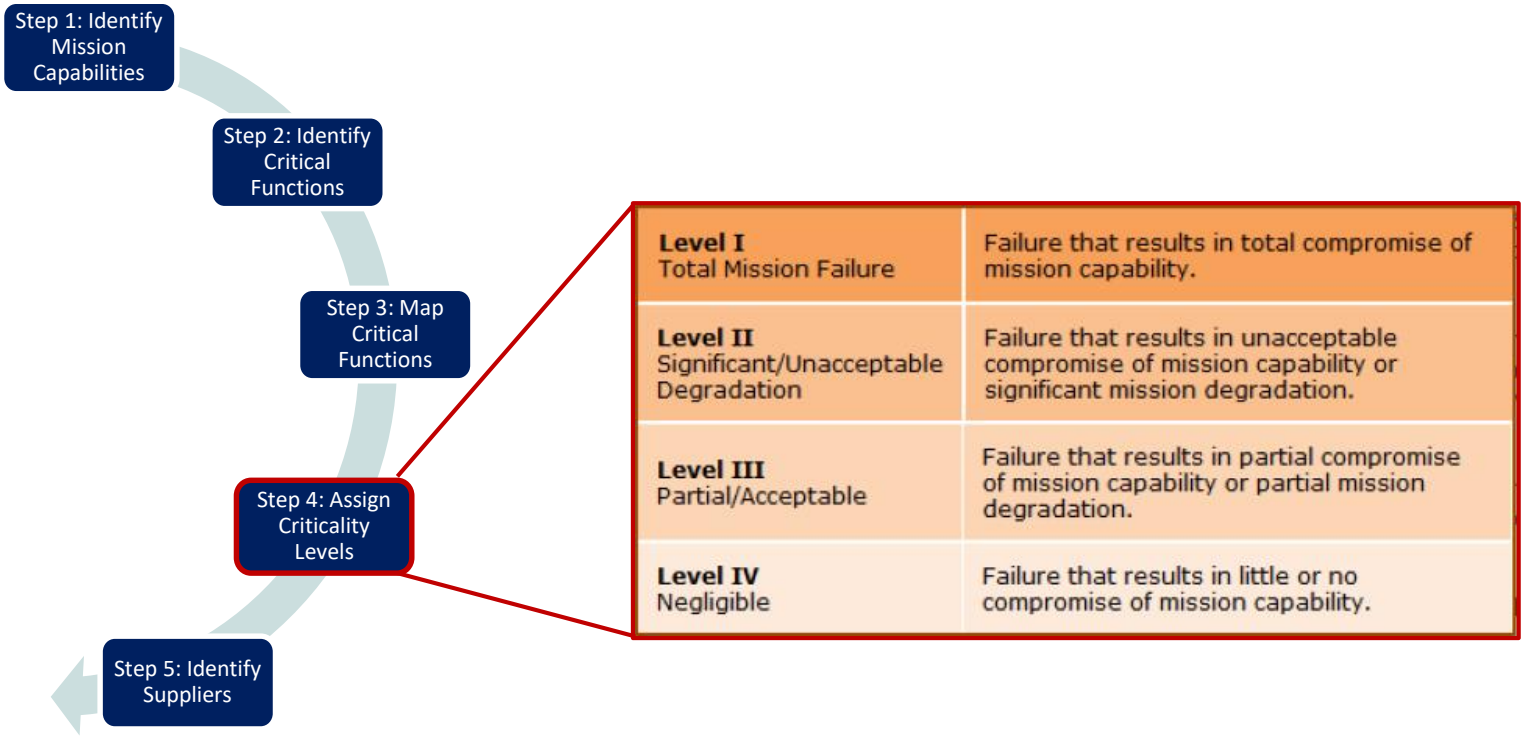
Implement SSE in design, development:
- Respond to SSE requirements
- Assess security risks during design review and system implementation

Verification & Validation

Conduct V&V:
- Evaluate AT protections
- Assess hardware and software vulnerabilities
- Verify SSE reqmts (Contractor, DT&E, OT&E)

Criticality Analysis

- **The primary method for a program to identify mission critical functions and components**
  - Mission-critical functions: “functions of the systems that, if corrupted or disabled, would likely lead to mission failure or degradation”
  - Mission-critical components: “primary elements (hardware, software, and firmware) of the system that implement mission-critical functions”
  - Only applies to information and communications technology (ICT)



Level I Total Mission Failure	Failure that results in total compromise of mission capability.
Level II Significant/Unacceptable Degradation	Failure that results in unacceptable compromise of mission capability or significant mission degradation.
Level III Partial/Acceptable	Failure that results in partial compromise of mission capability or partial mission degradation.
Level IV Negligible	Failure that results in little or no compromise of mission capability.

Many Supply Chain Risks Related to HwA to Consider

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

Anti-Tamper

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

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.

Emerging Threats

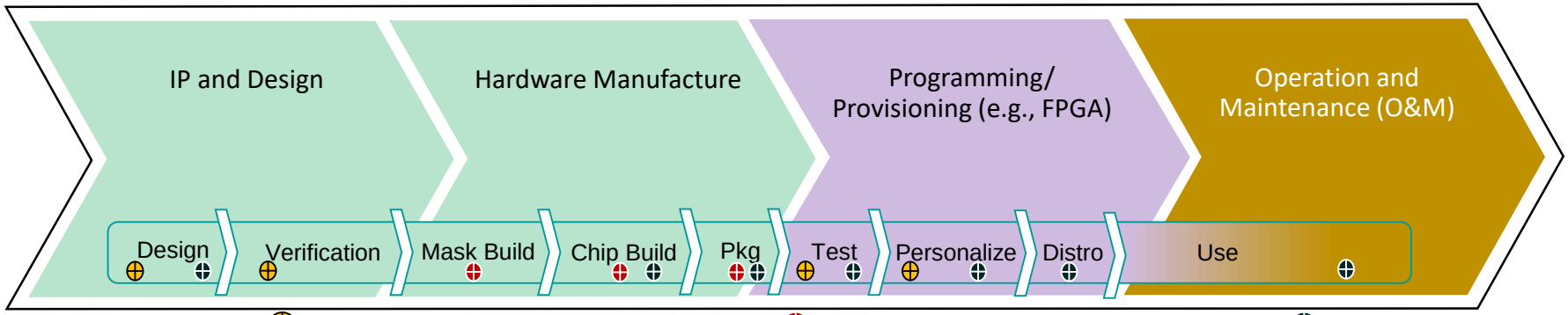
New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats

Proposition: Risk assessment approach must be integrated to address all

HwA Across the Lifecycle

HwA Lifecycle Risk/Mitigation

- **Assurance risks associated with HwA lifecycle phases include:**
  - Design risks: most closely associated with functions of the design process, Electronic Design Automation (EDA) tools, and intellectual property (IP)
  - Hardware risks: physical risks associated with hardware development and manufacture
  - Logistics risks: targeting of supply chain, to include transportation, counterfeit, theft, etc.



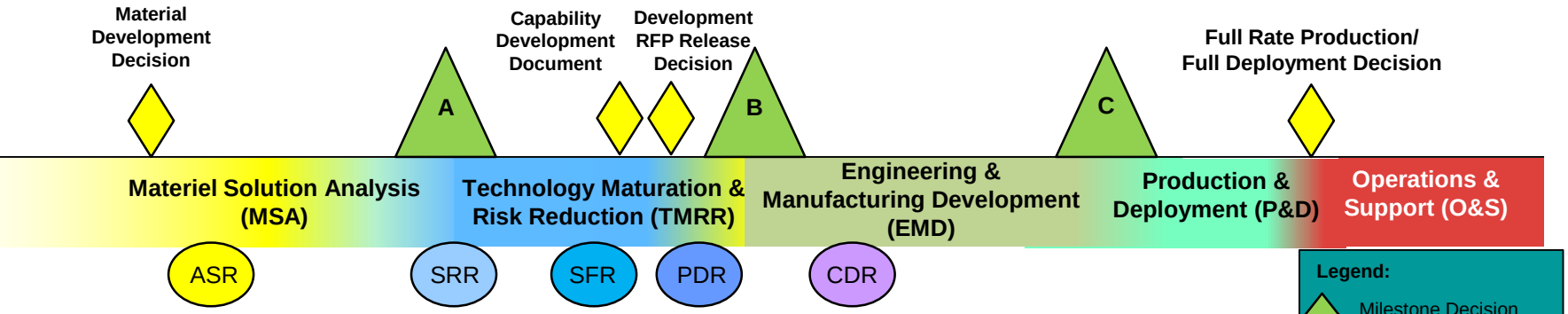
Design Risks	Mitigations	Hardware Risks	Mitigations	Logistics Risks	Mitigations
•Third party IP •EDA exploit •Insider modification •Security intercept •False expects, validation, test compares, bitstream	•IP/EDA Verification & Validation (V&V) •Cloud-based Secure Design Environment(s) (SDE), e.g., Trusted Silicon Stratus (TSS) •Cloud-based hardware/software emulation •Supply chain illumination	•Malicious insertion •Process compromise •Design for manufacturability (DFM) process exploitation •Package compromise	•Automated supply chain custody/ provenance tracking/access •V&V capability enhancements •Vendor/academic support of IP analysis/ assurance •Custom test/verification equipment	•IP theft •Overproduction •Hardware theft •Yield fail •Diversion •Counterfeit/cloning •Diminishing manufacturing sources and material shortages (DMSMS)/ obsolescence •Supply chain disruptions	•Defense Advanced Research Projects Agency (DARPA) supply chain hardware integrity for electronics defense (SHIELD) when available •Special handling of critical components •Vendor supply chain controls/access •GIDEP •Bulk buys •Parts banking

HwA Considerations for COTS CCs

- **Commercial off-the-shelf (COTS) components that perform critical functions require risk mitigation once end use becomes apparent to supply chain**
  - Acquire from Original Equipment Manufacturers (OEMs) or its authorized distributors
  - Maintain chain of custody control
  - For programmable logic devices, i.e., FPGAs, control device access and limit programming to cleared personnel
  - DLA sourcing decisions should be managed with program office engineering support
- **Employ supply chain risk management (SCRM) countermeasures**
  - See Key Practices and Implementation Guide for the DoD Comprehensive National Cyber Security Initiative 11 Supply Chain Risk Management Pilot Program
  - Obfuscate intended end by acquiring anonymously from OEM or authorized distributors
  - Employ anti-counterfeit business practices
  - Once fielded limit access/repair to cleared personnel
- **Networks and Information systems employ mostly COTS**
  - Cryptologic devices are most notable exception
  - Often acquired by DISA, GSA, and others as finished consumer products
  - From a HwA perspective, typically comprised of few if any CCs, although depending on criticality, its servers, routers and switches are potential targets for malicious insertion

HwA Across the Acquisition Lifecycle

- **Technology Development**
  - Document probable CCs and potential countermeasures
  - Plan life-cycle sustainment of proposed technologies



- **Engineering & Manufacturing Development**
  - Protect CCs by implementing appropriate techniques
- **Production & Deployment**
  - Control product baseline for Class 1 configuration changes
- **Operations & Support**
  - Manage CCs life-cycle and configuration

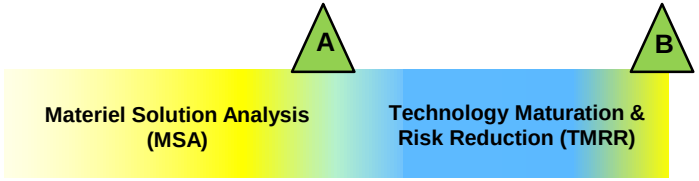
Configuration ➘ CDR ➘ Parts

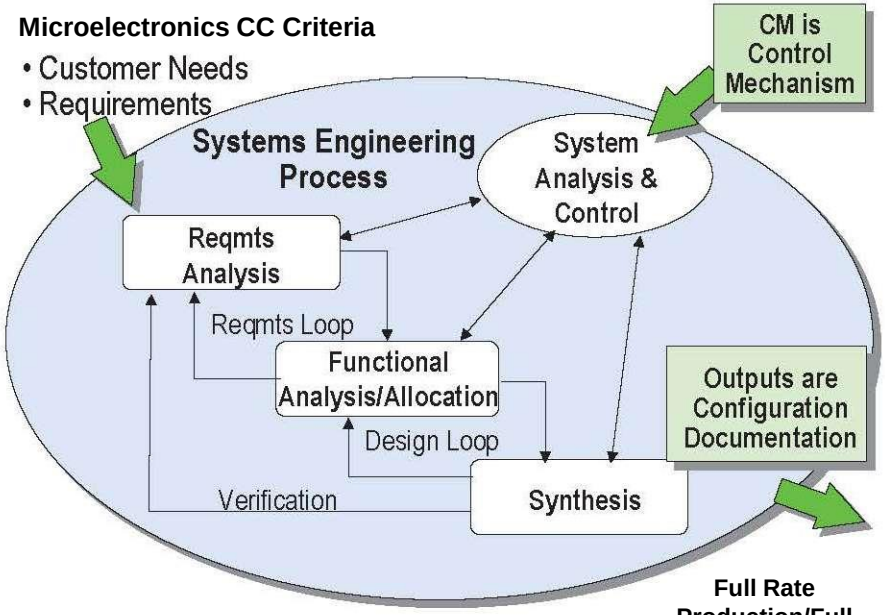
PPP Data/Info by Lifecycle Phase

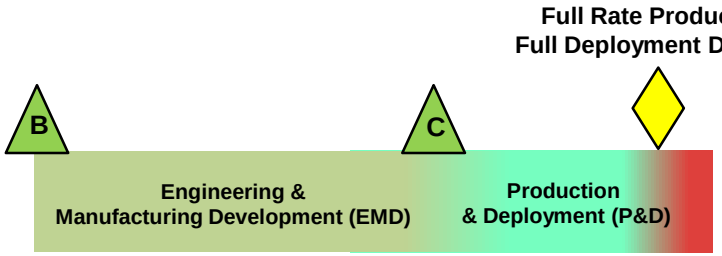
	Materiel Solution Analysis	Technology Maturation & Risk Reduction	Engineering & Manufacturing Development	Production & Deployment/ Operations & Support
Critical Functions/ CCs	System-level: Identify initial CCs, critical functions, and risk mitigation approach	System-level: Before PDR, ensure the identification of all critical functions, known CCs, and product risk mitigations. Component-level: For known Level I/II CCs, consider acceptance inspection/test to mitigate risk of malicious functionality and counterfeit insertion and/or other risk-based mitigations	System-level: Update HwA approach by CDR* identifying all CCs and risk mitigations. Post-CDR, conduct verification test for malicious functionality Component-level: For Level I/II CCs, consider acceptance test to mitigate risk of malicious code and counterfeit and/or other risk-based mitigations	System-level: Production and sustainment HwA approach to address maintenance for DMSMS concerns during and post-production Component-level: For Level I/II CCs, consider acceptance test to mitigate risk of malicious functionality and counterfeit and/or other risk-based mitigations
Supplier/ Supply Chain: -Systems Integrators, -Subsystem Manufacturers - CC Suppliers or Distributors	System-level: Identify initial suppliers, critical functions, and risk mitigation approach	System-level: Before PDR, identify process risk mitigations Component-level: 1. Establish component manufacturer qualifications for known CCs 2. Purchase from Original Component Manufacturers (OCMs) or authorized distributors whenever possible 3. Use anonymous procurement 4. Other risk-based mitigations	System-level: Updated supplier/supply chain approach before CDR, identifying risks and mitigations Component-level: 1. Customized CCs: assurance measures as required by DoDI 5200.44 2. Other CCs: Purchase from OCM or authorized distributor or DLA Qualified Manufacturer/Distributor 3. Anti-counterfeit procedures and inspections 4. Use anonymous procurement practice where practicable 5. Other risk-based mitigations	System-level: Production and sustainment HwA approach before FRP to include maintenance for DMSMS concerns during and post production Component-level: 1. Customized CCs: assurance measures as required by DoDI 5200.44 2. Other CCs: OCM/authorized distributor or DLA Qualified Manufacturer/Distributor with chain of custody for CCs 3. Anti-counterfeit procedures and inspections 4. Use anonymous procurement practice where practicable 5. Other risk-based mitigations

* CC= Critical Component, PDR = Preliminary Design Review, CDR = Critical Design Review, FRP = Full-Rate Production, DMSMS = Diminishing Manufacturing Sources and Material Shortages

Configuration Management (CM) Process







Microelectronics Controlled Items

- Initially tracked as CC functions
- Bill of materials populated as parts selection made
- Reporting to SE or Engineering Support Activity (ESA) for approval/management
- Special Procedures Code assignment

Full Rate Production/Full Deployment Decision

Operations & Support (O&S)

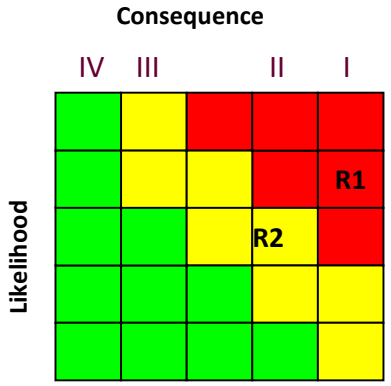
Parts Management

Life-Cycle Sustainment

- Organic Inventory Reassignment
- Contractor Logistic Support

DMSMS and HwA Risk

- **Any Integrated Circuit (IC) will have a long-term likelihood of becoming obsolete and/or commercially insupportable and/or unavailable**
  - For example, the likelihood of an aftermarket COTS IC being counterfeited or cloned is substantial (and highly targetable by adversaries)
- **Consequently, DMSMS risks to CCs, whether custom or COTS ICs and electronics assemblies, must be continually monitored and mitigations identified**

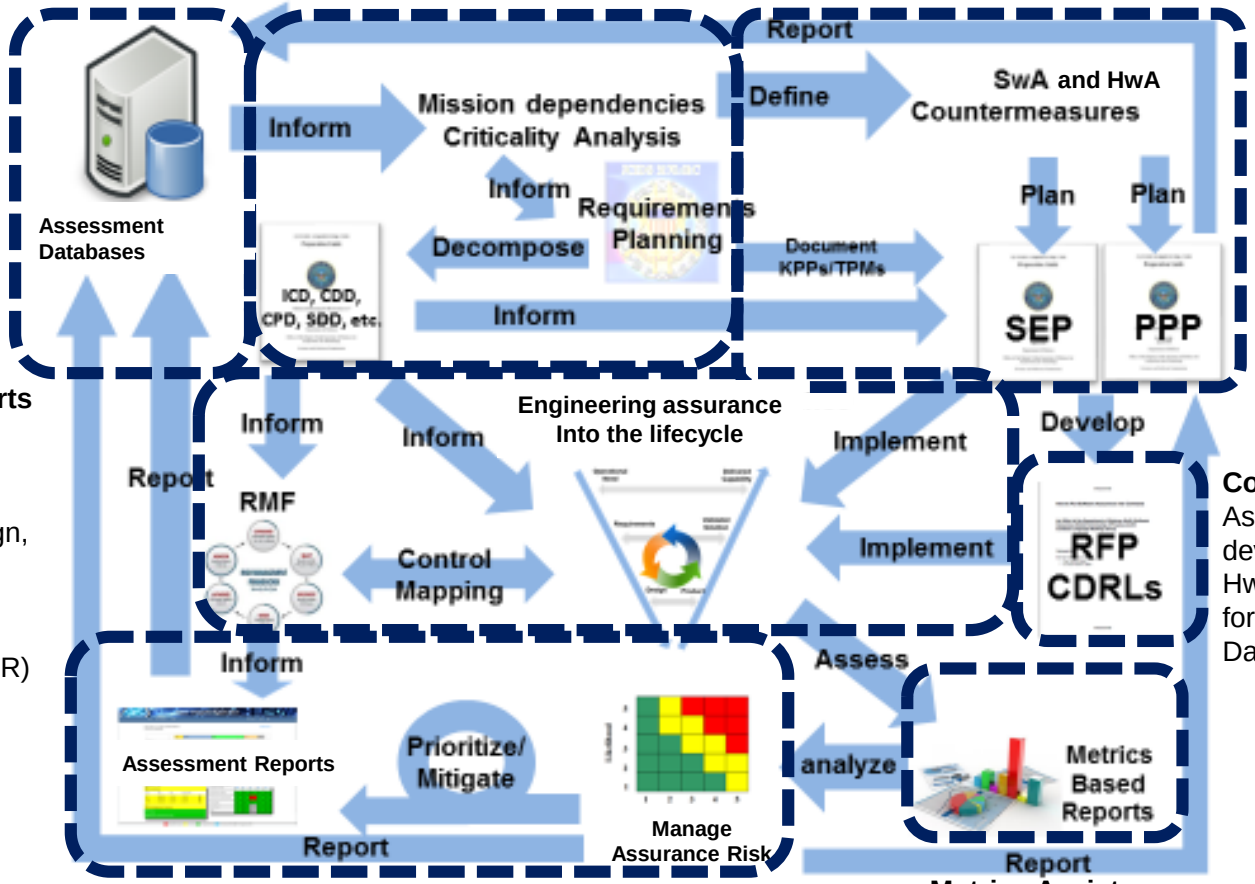


Joint Federated Assurance Center (JFAC) Support for HwA

JFAC Provider Capabilities

Software Assurance (SwA) and HwA Requirements Support:
Identification of applicable SwA and HwA requirements from policy, standards, instructions, and guidance

Knowledge Source:
Identification of applicable SwA and HwA assessments and attack information from assessment databases



PPP & SSE Planning:
Assistance with PPP development and the planning of SSE activities and countermeasures, to include SwA and HwA

Subject Matter Experts (SMEs):
SSE support during lifecycle, e.g., secure architecture and design, criticality analysis techniques, SCRM, system engineering technical review (SETR) criteria, sustainment support, etc.

Contract Assistance:
Assist programs with the development of SwA and HwA contract language for RFPs and Contract Data Requirements Lists

Third Party Assessment: Assistance in program evaluation and risk assessments, including bitstream analysis, hardware functional verification, static source code analysis, dynamic binary analysis, static binary analysis, web application analysis, database analysis, and mobile application analysis

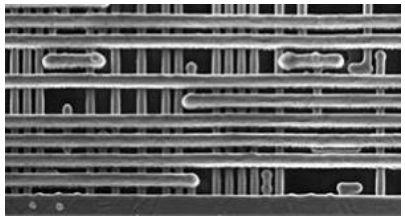
Metrics Assistance:
Assist programs with the identification, benchmarking, and collection of SwA and HwA related metrics (contract, progress, Technical Performance Measures, …)

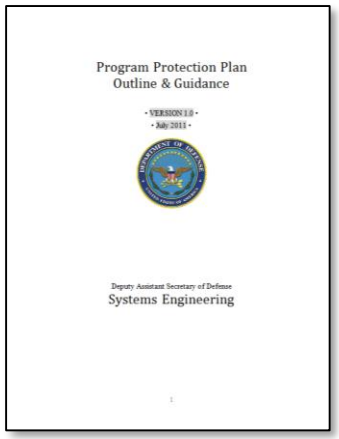
Example JFAC HwA Service Levels

Levels of Assurance		Standards & Best Practices	Modeling & Analysis	Hardware Assessment
Special or Program Specific	3		1 – JFAC Lab Design Verification	1 – JFAC Lab Physical Verification
Specialized JFAC Lab Service	2		2 – JFAC Design Simulations/ Modeling	2 – JFAC Lab Functional Verification
Core JFAC Lab Service			2 – JFAC SCRM Analysis	2 – JFAC Lab Functional Screening
Available for Primes (T&AM Provided & JFAC Vetted)		2 – JFAC Developed/Vetted Best Practices	2 – JFAC Developed/Vetted Tools	2 – JFAC Developed/Vetted Process
Base Assurance / Commercially Available (JFAC Vetted)	1	3 – Commercial/ Industry Standards (JFAC Vetted)	3 – Commercial/ Industry Tools (JFAC Vetted)	3 – Commercial/ Industry Process (JFAC Vetted)

Going Forward

Advance HwA





Enhance HwA

- Define levels of assurance and mitigations
- Identify attacks, and develop mitigations across the lifecycle (Not always 1-to-1 relationship)
- Establish/expand relationships with vendors in support of enhancing assurance of their products, e.g., co-development and/or vetting of next generation products, as well as their enterprise, e.g., SDEs
- Foster early acquisition program planning for HwA and SwA; design with security and assurance in mind

Focus and Align

- Collaboration with stakeholders to leverage and align FPGA assurance and broader related microelectronics and assurance initiatives
- Assess current investments and determine roadmap to address gaps
- Provide cloud-based secure design environments and consolidated knowledge and assessment repositories
- Enhance weapon system programs' connection to assurance community and industry
- Foster alliances with SwA and other SSE-related efforts
- Increase industry and commercial involvement for innovation in procedures, tools, and IP and standards development

Policy and Guidance

- Policy, guidance, and standards framework
- DoDI 5200.44
- New DoD Directive (DoDD) for Microelectronics
- PPP Outline and Guidance (O&G)
- HwA Program Managers Guide (PMG), including contracting language
- HwA Technical Implementation Guide (TIG)
- Industry-led commercial standards
- Alignment to industry standards, guidance and best practices

Supply Chain Assurance

- Supply chain assurance across lifecycle
- Bill of Material (BOM) analysis
- Component selection to increase DoD economies of scale and assurance
- Counterfeit/clone prevention
- DMSMS/obsolescence
- Handling of CCs in accordance with DoD Manual (DoDM) 4140.01, Volume 11
- Contracting language for SCRM, to include flow-down to subs

Program Engagement

- **Support USG acquisition and weapon system programs incorporation of assurance:**
  - Implement expectations in requirements, planning, and contracting
    - Define formal levels of assurance and associated protection
  - Provide more comprehensive guidance in contracting language
    - For example, support "acquire to verify" – ensure that programs and contractors (prime and sub) consider information or data acquisition that provide the USG information needed for verification and validation or future Operations and Maintenance support
  - Foster early planning for HwA and SwA; design with security and assurance in mind
  - Communicate strategy to programs for common articulation of vulnerabilities and weaknesses, capabilities, and countermeasures
  - Ensure FPGA/System on Chip (SOC) (and all microelectronics) assurance is supported in PPP
  - Provide access to JFAC and discipline specialists throughout the lifecycle, e.g., SETRs

Industry Engagement

- **Leverage industry, to include FFRDCs and associations, and academia**
  - Develop policy and guidance for common articulation of vulnerabilities and weaknesses, capabilities and countermeasures
  - Co-development of next generation COTS with DoD capabilities and assurance considered
  - Industry-led development of commercial standards to be implemented by vendors for assurance of both supply chain and components
  - Ensure DoD strategies – including microelectronics and FPGAs/SOCs – can evolve in practical relationship with the commercial sector
  - Explore vendor-driven standards and best practices that can positively support DoD interests and requirements
  - Engage industry to create new tools and upgrade existing ones to support easier formal V&V and synthesis verification options
  - Collaborate in IP vetting efforts and working towards access-controlled third party IP repository
  - Establish stronger JFAC-vendor relationships that allow access to design, manufacturing details, and revision data to ensure JFAC remains technically current

Government Engagement

- **Example USG engagements include:**
  - DoD Trusted and Assured Microelectronics (T&AM)/Microelectronics Innovation for National Security and Economic Competiveness (MINSEC)
  - JFAC Service Providers
  - Defense Advanced Research Projects Agency programs
  - Printed Circuit Board and Interconnect Technology Executive Agent related technology development
  - Intelligence Advanced Research Projects Activity programs
  - Strategic Radiation-Hardened Electronics Council (SRHEC)
  - Nuclear Enterprise Assurance Steering Group (NEASG)
  - Office of Management and Budget and other White House-sponsored activities

There are many USG, industry, and academic efforts in this and related areas to leverage

DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow










DoD Research and Engineering Enterprise
https://www.acq.osd.mil/chieftechnologist/

Defense Innovation Marketplace
https://defenseinnovationmarketplace.dtic.mil

Twitter
@DoDInnovation

For Additional Information

Ray Shanahan

Office of the Under Secretary of Defense
Research and Engineering
571-372-6558 | raymond.c.shanahan.civ@mail.mil