



ACQUISITION OF SOFTWARE-DEFINED HARDWARE-BASED ADAPTABLE SYSTEMS

Andrew Hunter

May 8, 2019

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

International
Security Program

II. Overview (1/2)

- Future success is dependent on ability to adapt and rapidly adjust to uncertainties in threats, nimble adversaries, rapidly emerging (and obsolescence of) technologies, and new domains.
- Commercial technology and processes have advanced toward more continuous, iterative software development that can harness technology advances, continuous upgrade, utilize machine learning, and better leverage user-feedback.
- DoD must look for ways to harness this innovation and incorporate smarter solutions for defense through acquisition and modification of systems that are multifunctional and designed for continuous modification



“Simply delivering what was initially required on cost and schedule can lead to failure in achieving our evolving national security mission — the reason defense acquisition exists in the first place.”

*Hon. Frank Kendall Under Secretary of Defense (AT&L)
2015 Performance of The Defense Acquisition System*

II. Overview (2/2)

- **Adaptable Systems are defined as hardware-based, software-intensive systems**
- **They are:**
 - Distinct from systems that are simply modular (able to add additional capability packages) or reconfigurable (able to be physically modified between missions to alter functionality)
 - Able to deliver many capabilities from a single basic design (multifunctionality) and add capability over time (growth) at speed of relevance (cycle time less than 2 years).
 - Relevant to both upgrade and sustain existing systems as well as establish design for new systems and platforms



Photo: Flickr/US Air Force

III. Examples

<p>Battlefield Airborne Communications Node (BACN) /Global Hawk</p>	<p>Operational Control System (OCX)</p>	<p>Surface Electronic Warfare Improvement Program (SEWIP)</p>
<ul style="list-style-type: none"> • Loose integration, acceptance of off-the-shelf materials • Trade-offs to provide near-term solution • Budgeting and resources for limited beneficiaries • Mismatch between incentives and constraints on funders and beneficiaries 	<ul style="list-style-type: none"> • Criticality of cyber defenses, needed to be designed to address these from ground up • Rapidity of change in defensive capability • Need strong foundational base even while trying to streamline process • Program ownership and management difficulties • Budget estimates and delays 	<ul style="list-style-type: none"> • Need to adapt rapidly and constantly to adversaries' offensive and defensive capabilities • Need to adapt and change at sea (Upgrade on the Go) • Challenge of making and meeting budget & schedule estimates • Importance of collaboration and increased partner interaction in defining architecture

IV. Barriers

- **MDAP structure (30 year planning and focus on rate production, EVMS)**
- **Limited/Late User Feedback/Organizational Culture (Pass/Fail Oversight and Test)**
- **Resource Ownership (Budgeting around MDAPs, Colors of Money)**
- **Misaligned Business Incentives (Legal Barriers and Proprietary IP)**
- **Workforce/Technical Expertise (MOSA/Software Acquisition, etc)**

V. Enablers

- **Adaptable architectural designs (MOSA)**
- **Incremental and iterative development**
 - *Agile, DevOps, Virtual Twin testing, Sprints*
- **Continuous T&E/Dynamic User Feedback**
- **Dynamic Marketplace**
- **Budgeting for Adaptability**
- **Flexibility in Funding and Contracting**
- **Increased user/customer interaction, feedback loops**
- **Functionally aligned workforce & training**

V. Turning Enablers Into Solutions

- **Create an Adaptable Systems pathway where use of the key enablers is the norm**
 - Enablers are not exclusive to the pathway
 - Enablers are not mandatory
- **Develop a cadre of Adaptable Systems experts in the workforce**
 - Requires as much effort on the requirements and budgets side as on the acquisition side

VII. Closing Remarks

I. Backup Slides