Securing Warfighting Systems in a Net-Centric Environment

Lt Col Brett Telford
Deputy Director

Open Systems Joint Task Force/OUSD (AT&L)
(703) 602-0851 X116, FAX 602-3560,
e-Mail: kenneth.flowers@osd.mil
www.acq.osd.mil/osjtf

27 April 2006

Net-Centric Warfare

- *Net-Centricity* is a transformation enabler that empowers all users with the ability to easily discover, access, integrate, correlate and fuse data/information that support their mission objectives.

- The transition to net-centric warfare brings with it a number of challenges:
  - Operational
  - Technology and Design
  - Acquisition
  - Business

- Perhaps the most taxing challenge is how to affordably secure our systems in this new networked environment
  - Must balance “need to share” with “need to know”
  - Must address needs of allied and coalition partners as well as other agencies (e.g., “First Responders”)

USD(AT&L) Imperative

I should note … that we have taken important steps that will help us to produce improved capability on time and within budget by re-energizing our approach to systems engineering. This critical discipline has always contributed significantly to effective program management at every level and will receive sustained emphasis during my tenure.

Testimony of The Honorable Kenneth J. Krieg, USD(AT&L), before US Committee on Armed Services, September 27, 2005

Addressing The NCW Challenge

- The Modular Open Systems Approach (MOSA) provides a solid systems engineering foundation upon which to address NCW challenges
- DoD is developing, demonstrating, and transitioning “transformational” embedded information technologies to facilitate insertion of new capability into fielded systems to:
  - ✓ Incrementally migrate **closed** architectures to more capable **open systems architectures** (i.e., hardware, software, models)
  - ✓ Utilize industry middleware standards and emerging resource management technologies to provide “internet-like” protocols over existing data links for fielded systems
  - ✓ Leverage advances in information technology to incorporate new capability to support integration with emerging platforms
  - ✓ Address emerging challenges (i.e., security, machine-to-machine communications)

A Real-World Application of Open Systems

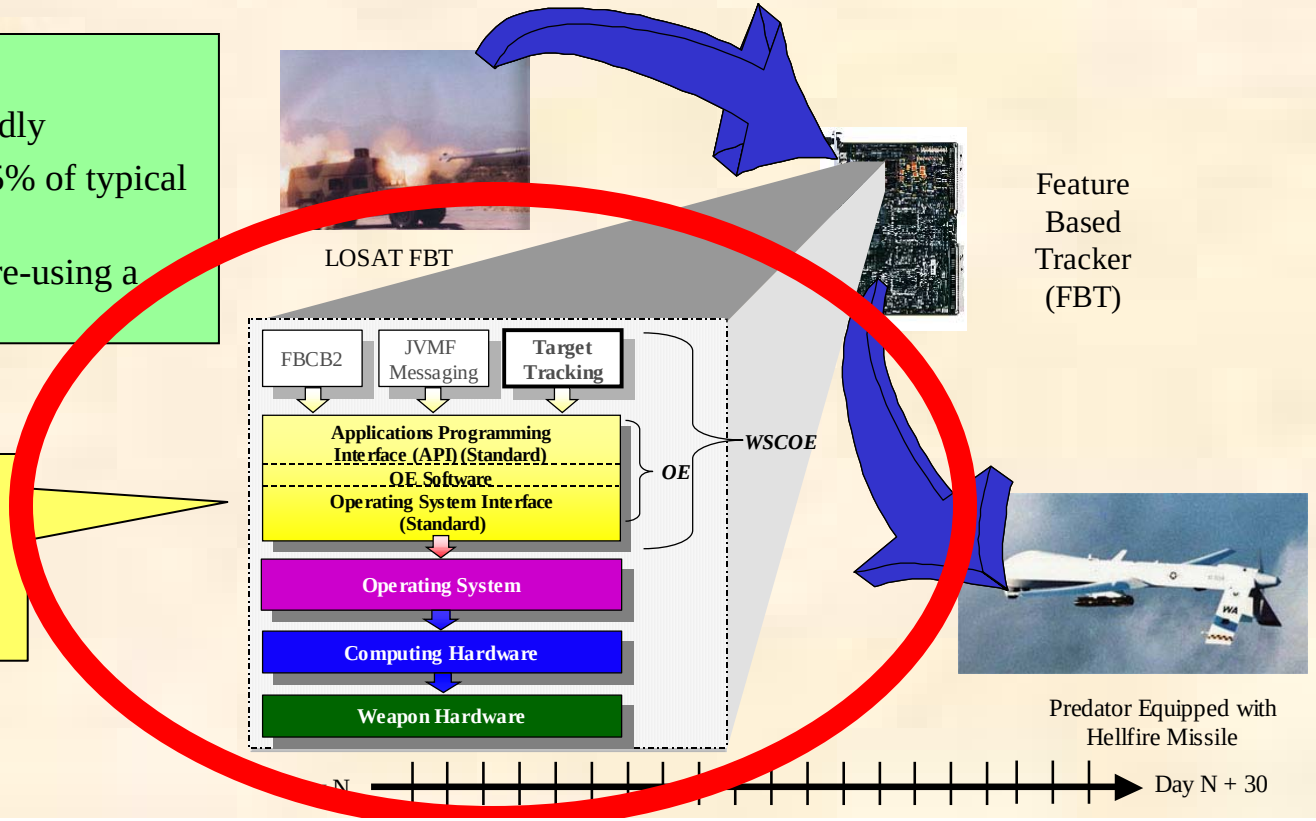
- What
  - Predator UAV was augmented with Hellfire missile in just over 30 days for rapid deployment in Afghanistan.
- How
  - Critical target tracking software was easily rehosted from LOSAT (Line of Sight Anti-Tank) computing environment to Predator's because it was built upon the Army's open Weapon System COE API.
  - The WSTAWG COE specifies common services for managing the 1553 bus and for handling digital video.

Resulted in:

- A New Capability - fielded rapidly
- Significant Cost Avoidance - 75% of typical software development costs
- Enhanced Interoperability - by re-using a proven weapon systems product

Enabled by MOSA using:

- Modular Design
- Key Interfaces
- Open Standards



The Way Ahead for Security Architectures

MILS collaborative efforts are to be commended:

- Broad participation across DoD, technology developers, systems integrators, academia and COTS vendors
- On right track to achieve consensus standards & profiles
- High potential to substantially reduce certification costs and schedules
- Can achieve on-going savings by leveraging commercial developments underpinned by purpose-built infrastructure

MILS can fulfill a critical need in legacy and future defense systems

Open Systems

OS

Joint Task Force