Overcoming the Government-Industry Collaboration Obstacles

Patrick J. Martin, Ph.D.
Sr. Principal Research Engineer
patrick.j.martin@baesystems.com
Technology Solutions

10-26-2017

© 2017 BAE Systems

2017 NDIA Systems Engineering Conference

BAE SYSTEMS
INSPIRED WORK

The Future of System Development
Rapidly Evolving Threats

Technology is democratized

OpenStack

AWS

Raspberry Pi

BitBucket

Github

ArduPilot

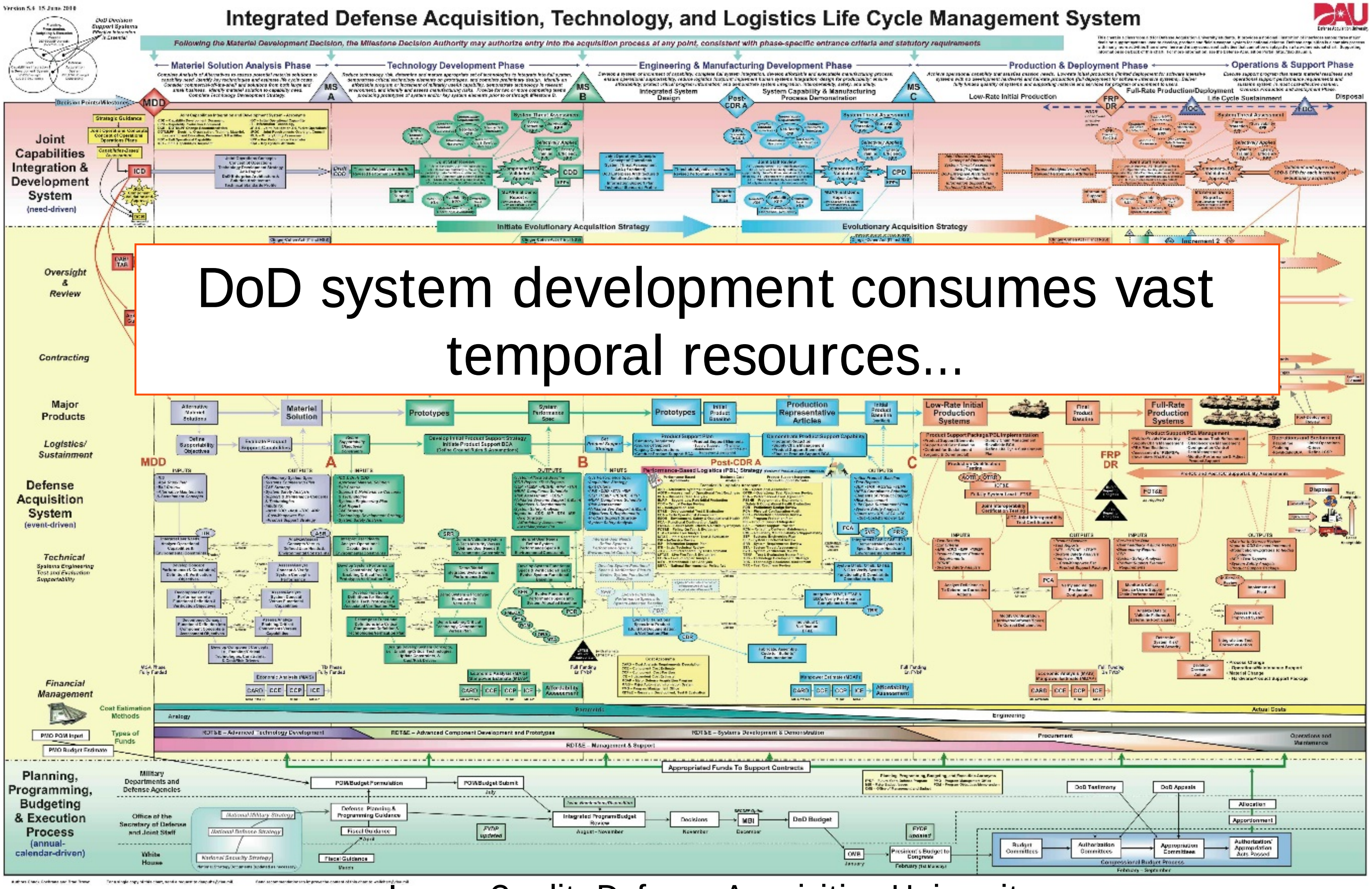
OpenSource Hardware

OpenRobotics

Near-peer and insurgent adversaries rapidly adapt tools and tactics

© 2017 BAE Systems

The Future of System Development
Unsustainable Processes


Version 5.4 15 June 2010
Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System
Following the Materiel Development Decision, the Milestone Decision Authority may authorize entry into the acquisition process at any point, consistent with phase-specific entrance criteria and statutory requirements
Materiel Solution Analysis Phase
Technology Development Phase
Engineering & Manufacturing Development Phase
Production & Deployment Phase
Operations & Support Phase
MDD
MS A
MS B
MS C
Post-CDR A
FRP DR
Integrated System Design
System Capability & Manufacturing Process Demonstration
Low-Rate Initial Production
Full-Rate Production/Deployment
Life Cycle Sustainment
Disposal
IOC
FOC
Joint Capabilities Integration & Development System (need-driven)
ICD
CDD
CPD
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition Strategy
Oversight & Review
Contracting
Major Products
Materiel Solution
Prototypes
Production Representative Articles
Low-Rate Initial Production Systems
Full-Rate Production Systems
Logistics/ Sustainment
Defense Acquisition System (event-driven)
Technical
Financial Management
Cost Estimation Methods
Types of Funds
Analogy
Parametric
Engineering
Actual Costs
RDT&E – Advanced Technology Development
RDT&E – Advanced Component Development and Prototypes
RDT&E – System Development & Demonstration
RDT&E – Management & Support
Procurement
Operations and Maintenance
Appropriated Funds To Support Contracts
Planning, Programming, Budgeting & Execution Process (annual-calendar-driven)
Military Departments and Defense Agencies
Office of the Secretary of Defense and Joint Staff
White House
POM/Budget Formulation
POM/Budget Submit
Defense Planning & Programming Guidance
Fiscal Guidance
Integrated Program/Budget Review
Decisions
MBI
DoD Budget
President's Budget to Congress
DoD Testimony
DoD Appeals
Budget Committees
Authorization Committees
Appropriation Committees
Authorization/ Appropriation Acts Passed
Allocation
Apportionment
Congressional Budget Process
DAU

DoD system development consumes vast temporal resources...

Image Credit: Defense Acquisition University

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

The Future of System Development
Unsustainable Processes

...and time IS money.

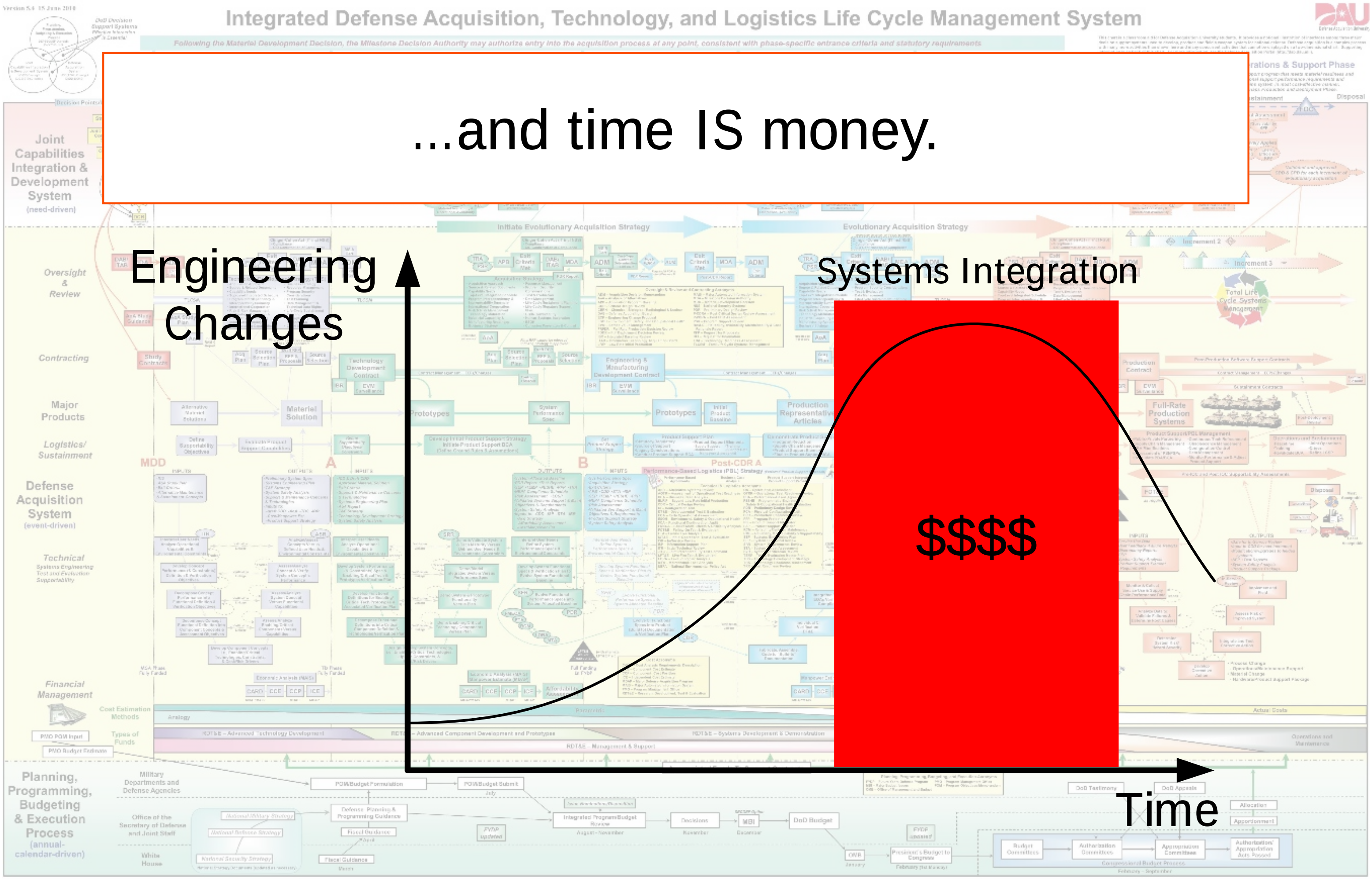


Image Credit: Defense Acquisition University

© 2017 BAE Systems

The Future of System Development

Developing, testing, and deploying engineered resilient systems will require **collaboration** across the DoD community

Technological Hurdles

- Security
- Scalability
- Flexibility

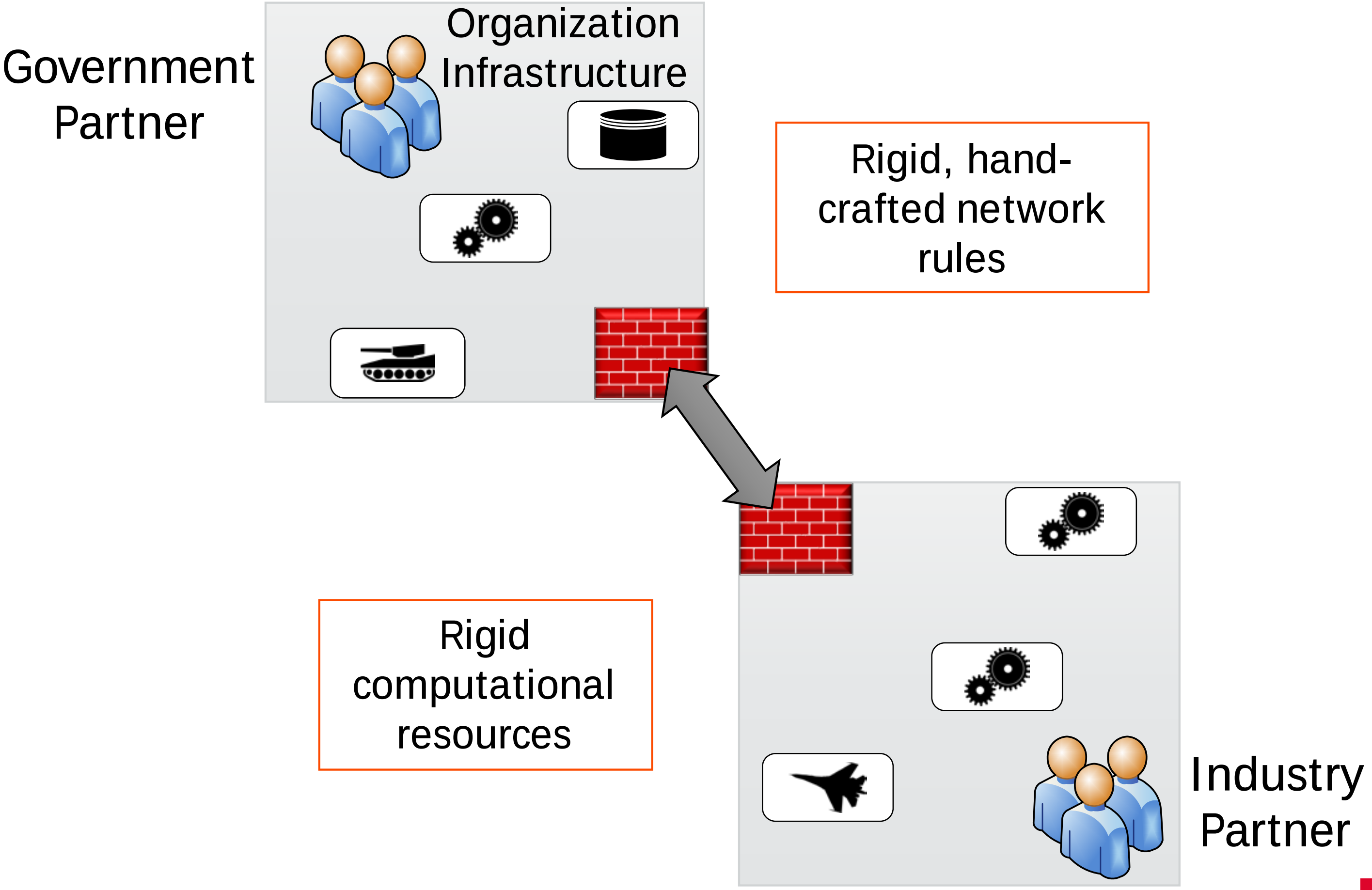
Policy Hurdles

- Security
- Legal
- Business

© 2017 BAE Systems

Collaboration Challenges

Partner collaboration is ad-hoc
Multiple IT and security organizations involved



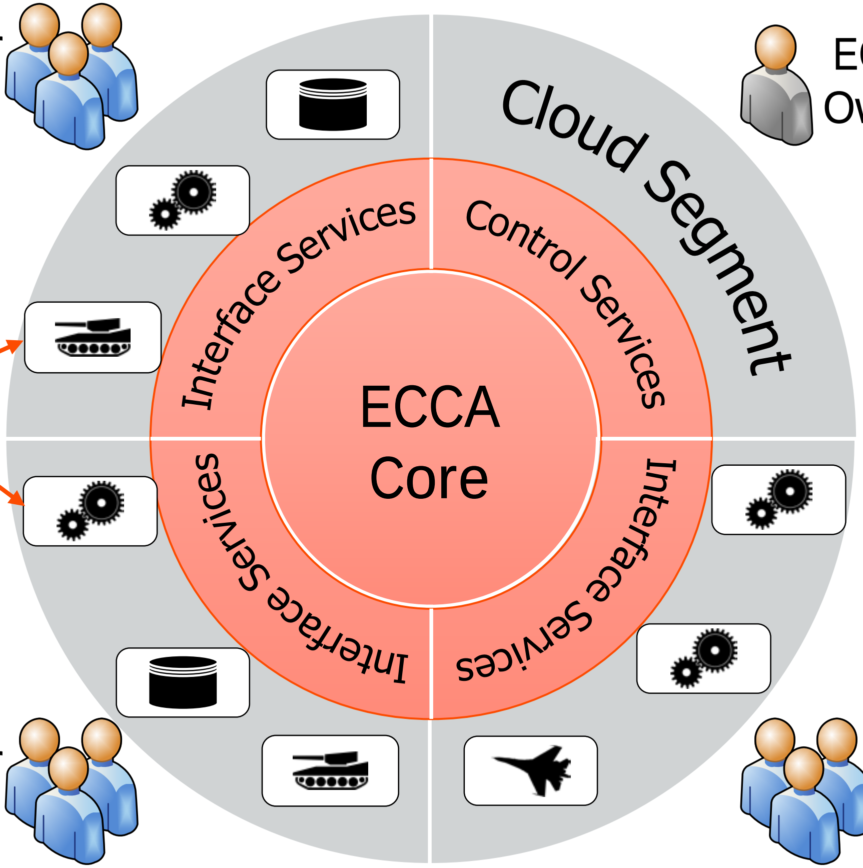
Rigid, hand-crafted network rules

Rigid computational resources

© 2017 BAE Systems

ERS Cloud Computing Architecture (ECCA)

ECCA provides a **collaborative analysis environment** for industrial, academic, and government partners



Dynamically scalable assets

Flexible networking rules

© 2017 BAE Systems

ERS Cloud Computing Architecture (ECCA)

Benefits and **Risks**

What we want...

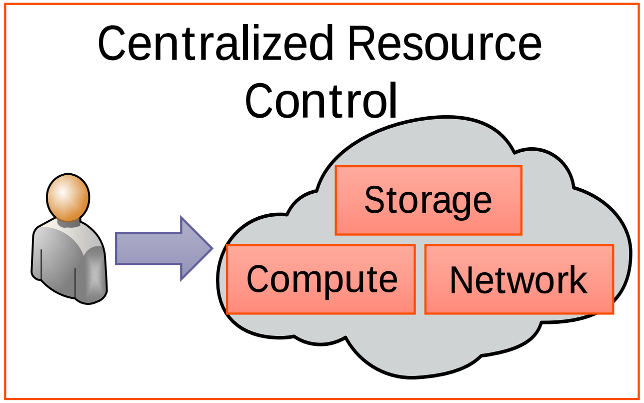
- Controlled access to M&S capabilities
- “Programmable” analysis applications
- Rapid capability sharing with DoD customers
- Discovery of strategic partners

What we need to worry about...

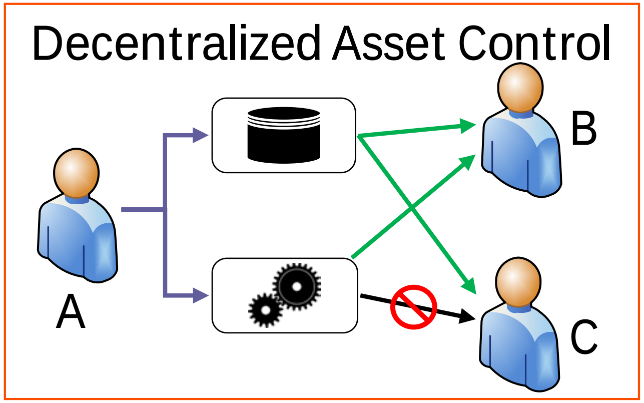
- Standard network security risks
- IP Leakage, Side channel exfiltration
- Malicious assets
- Cloud computing resource overrun

© 2017 BAE Systems

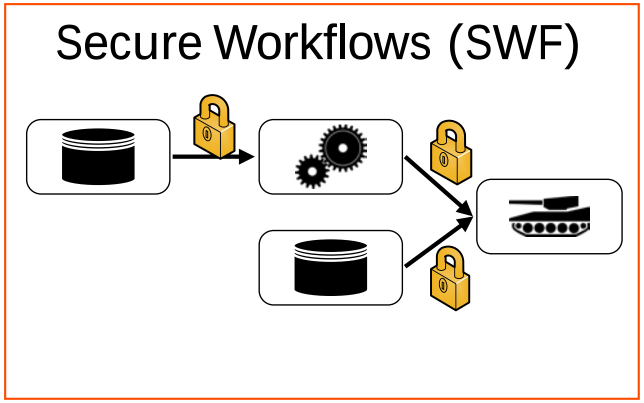
ECCA High Level Concepts



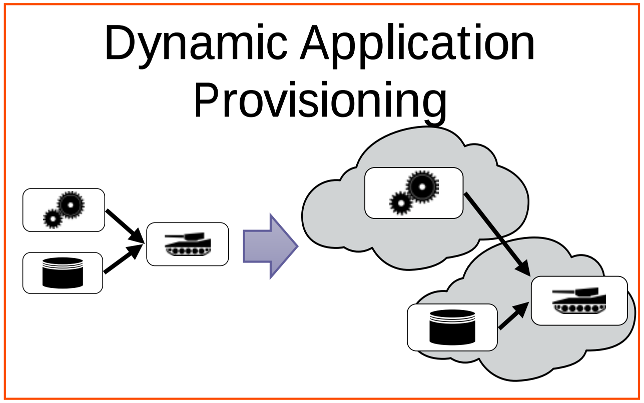
Centralized Resource Control



Decentralized Asset Control



Secure Workflows (SWF)

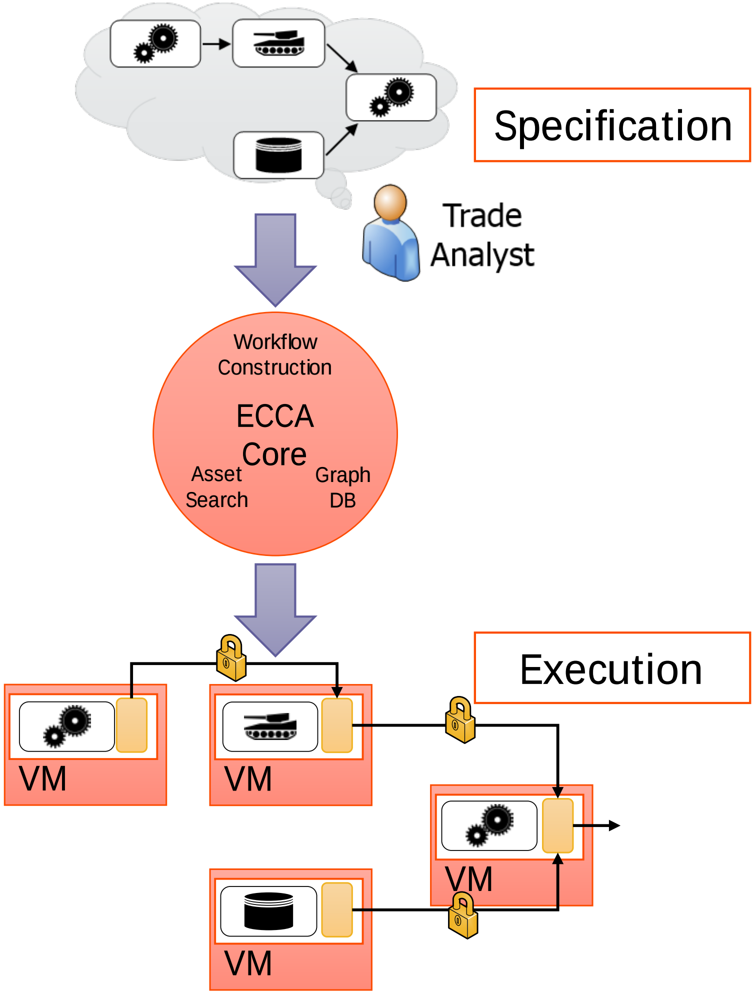


Dynamic Application Provisioning

© 2017 BAE Systems

ECCA IP Protection Strategy

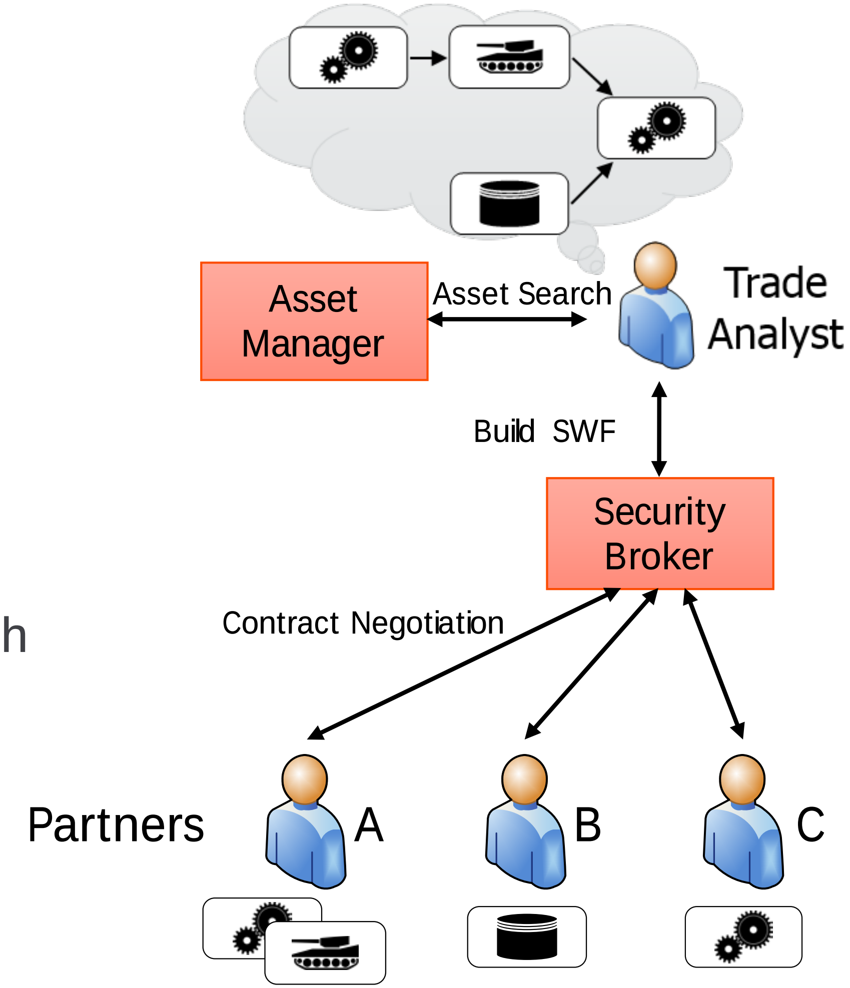
- Encryption at-rest and in-motion
- Partners locally control access to their M&S assets
- Leverage recent cloud computing advances to enable:
  - Isolation of runtime assets
  - Automatic generation of secure software defined networks



© 2017 BAE Systems

Secure Workflows

- AoA applications involve multiple organizations and their assets
  - Interactions must be agreed upon by the entities involved
- The Secure Workflow (SWF) is:
  - A model of an authorized analysis application...
  - ...where assets are attached with limits set by Asset Owners (e.g. call limit, timing)



© 2017 BAE Systems

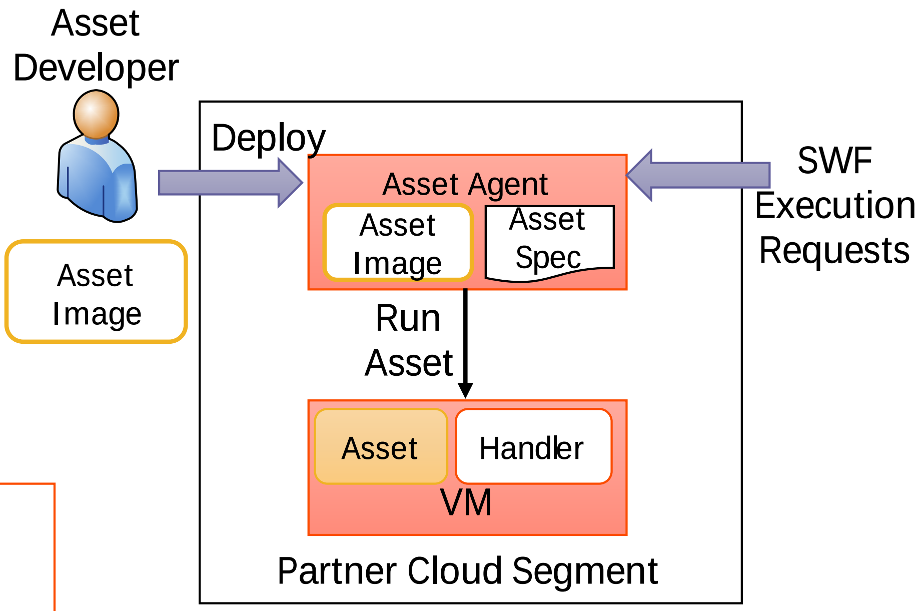
ECCA Asset Management

- Challenges:
  - Assets are heterogeneous
  - Assets could be malicious
  - ...but still need collaboration
- ECCA Solution: Asset Agents

Maintain asset containers

Publish asset meta-data

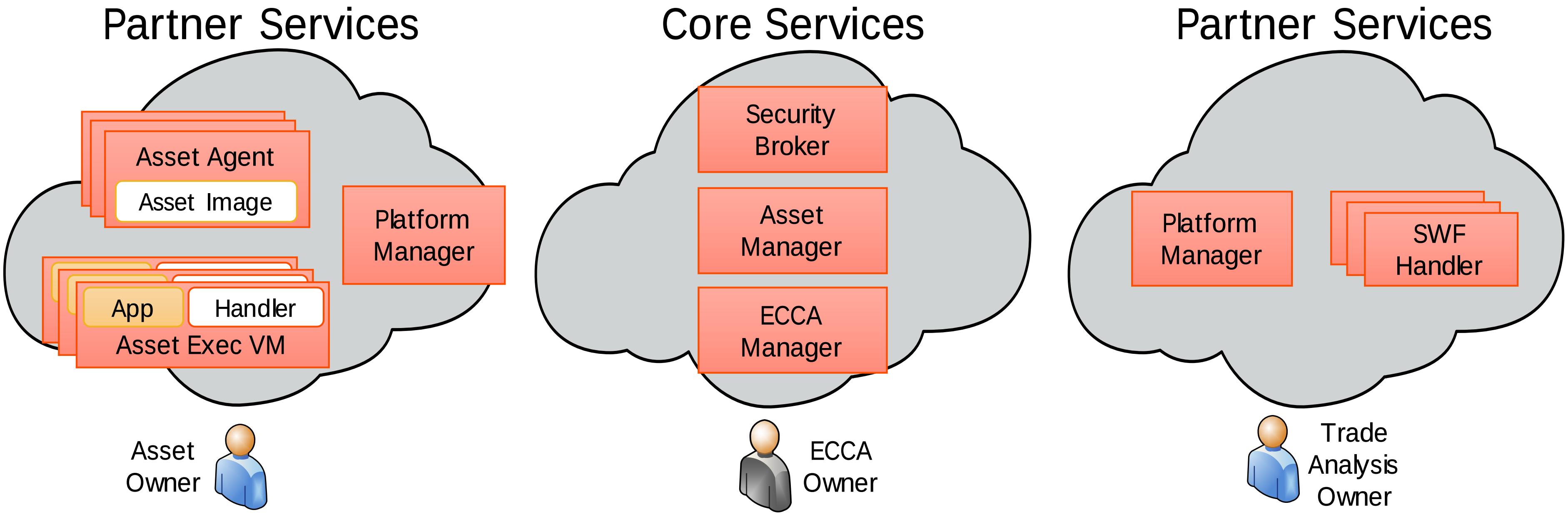
Isolate with automatically generated handlers



© 2017 BAE Systems

ECCA Design

Distributed, Micro-service Architecture



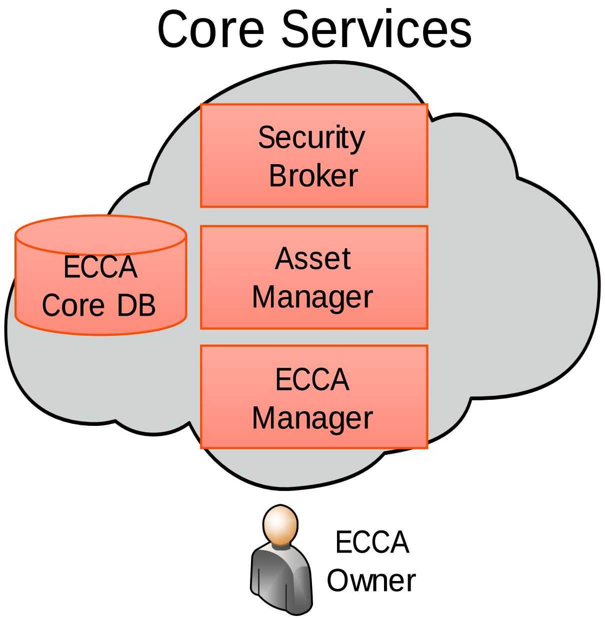
ECCA services manage cloud segment federation

© 2017 BAE Systems

ECCA Design
Core Services

Security Broker

- Manages allowed ECCA entities in graph DB
- Orchestrates the SWF execution



Asset Manager

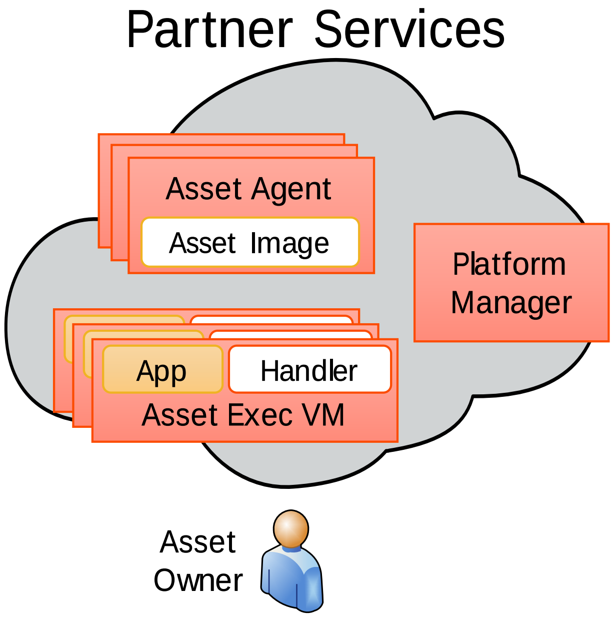
- Facilitates asset meta-data searches in the ECCA Core DB

ECCA Manager

- Controls allowed Partner organizations
- Controls resources available for AoA applications

© 2017 BAE Systems

ECCA Design
Partner Services: Asset Management



Platform Manager

- Interfaces to ECCA
- Enables peering among other Partner cloud segments
- Enables Asset publishing

Asset Agent

- Maintains a Partner asset within their cloud segment

Asset Execution Infrastructure

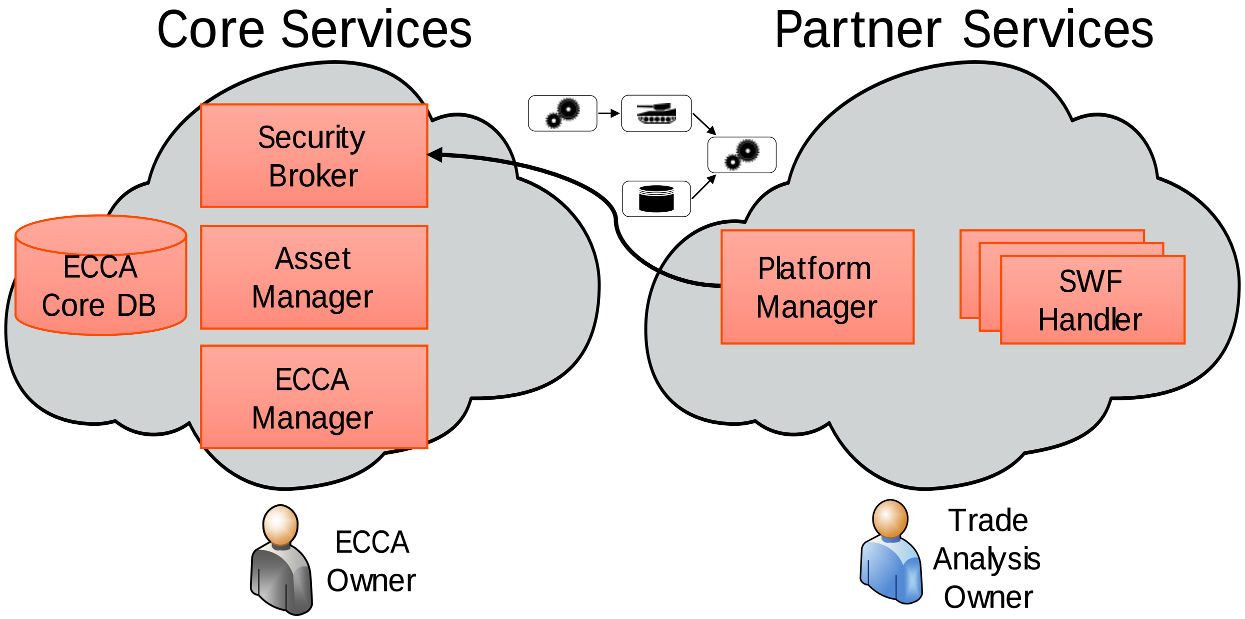
- Virtual Machine(s) execute Asset App
- Handler service isolates Asset App
- Supervisor manages Asset Apps based on SWF constraints

© 2017 BAE Systems

ECCA Design
Partner Services: SWF Management

Platform Manager
- Maintains SWF with the Security Broker

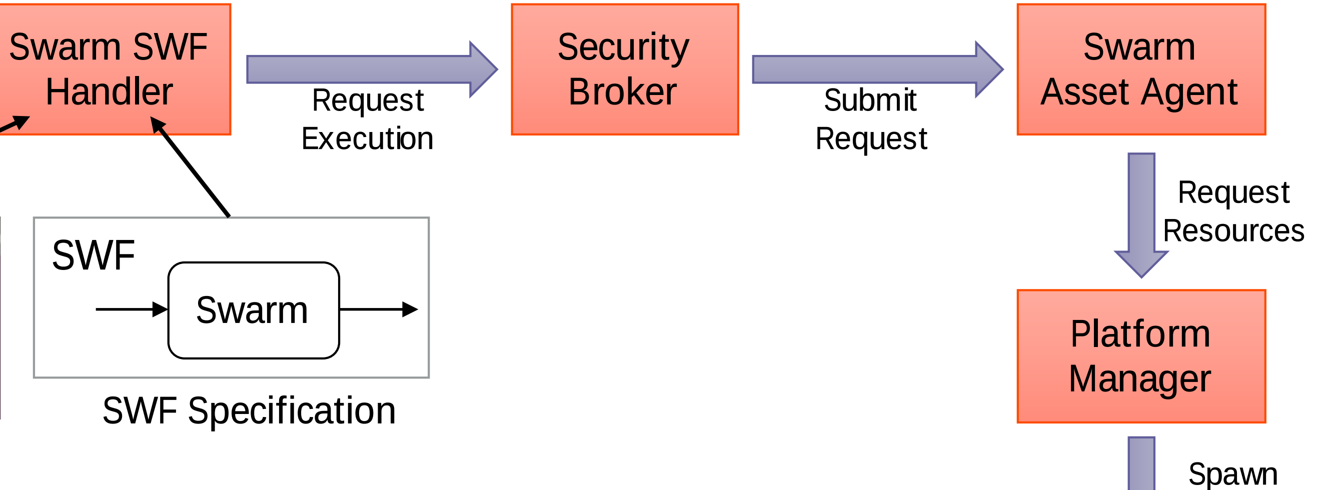
SWF Handler
- Enable construction of SWF from deployed assets within ECCA
- Submit initial data and received SWF results



© 2017 BAE Systems

ECCA Program Status

ECCA lab prototype is live…



ERDC Analyst

Swarm SWF Handler

Request Execution

Security Broker

Submit Request

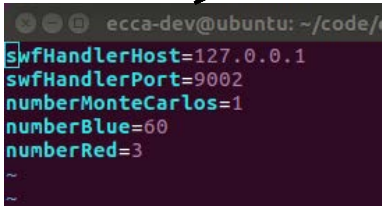
Swarm Asset Agent

Request Resources

Platform Manager

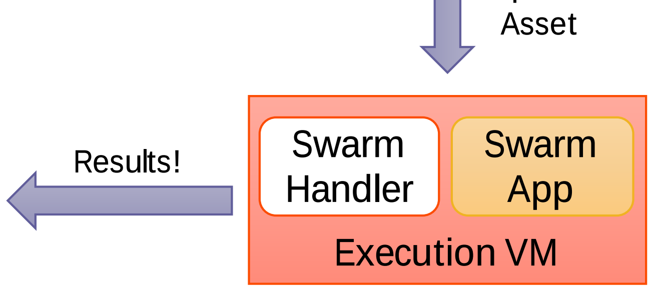
Spawn Asset

SWF Specification



```
swfHandlerHost=127.0.0.1
swfHandlerPort=9002
numberMonteCarlos=1
numberBlue=60
numberRed=3
~
~
```

Initial Conditions

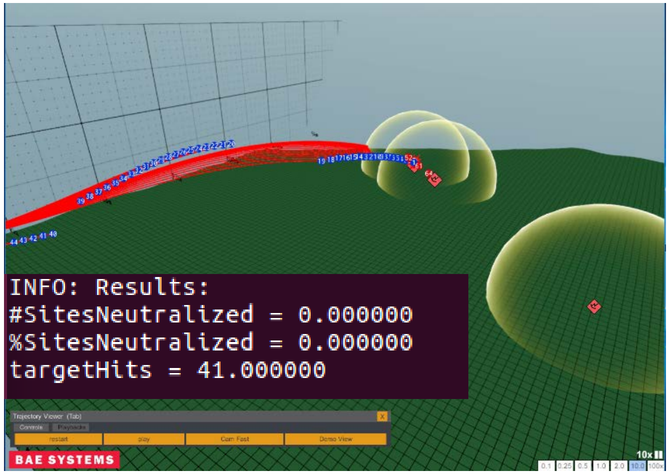


Swarm Handler

Swarm App

Execution VM

Results!



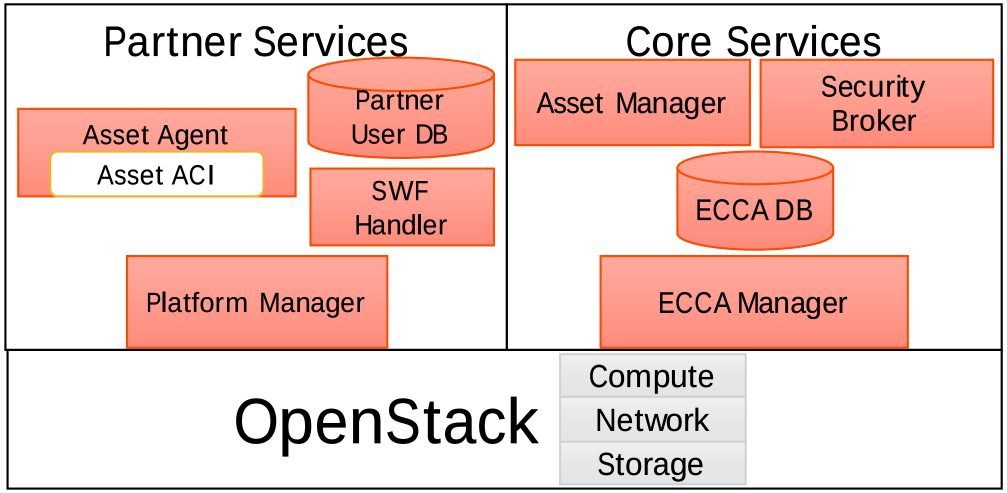
```
INFO: Results:
#SitesNeutralized = 0.000000
%SitesNeutralized = 0.000000
targetHits = 41.000000
```

© 2017 BAE Systems

ECCA Program Status

...more work remains to go to prime time!

Integration and test on OpenStack:



Further R&D:

Cross Cloud Peering Mechanisms

Commercial Tool Integration

“ERS Language”

Asset Reputation and Trust

© 2017 BAE Systems

BAE SYSTEMS
INSPIRED WORK

Conclusion

- Dynamic threats call for rapid DoD system design, test, and evaluation processes.
- ECCA is the first step to facilitate secure collaboration among DoD partners.
- This collaborative environment will provide tools for decision makers and engineers to develop, assess, and (re)engineer resilient systems.

© 2017 BAE Systems

Acknowledgements

- The ECCA Team:
  - Brent Baker, Collin Blakley, Greg Eakman, Rob Ross, Bill Sexton, Chris Wentland

- This research effort was funded by the US Army Corp of Engineers ERDC

© 2017 BAE Systems

Thank you!

© 2017 BAE Systems