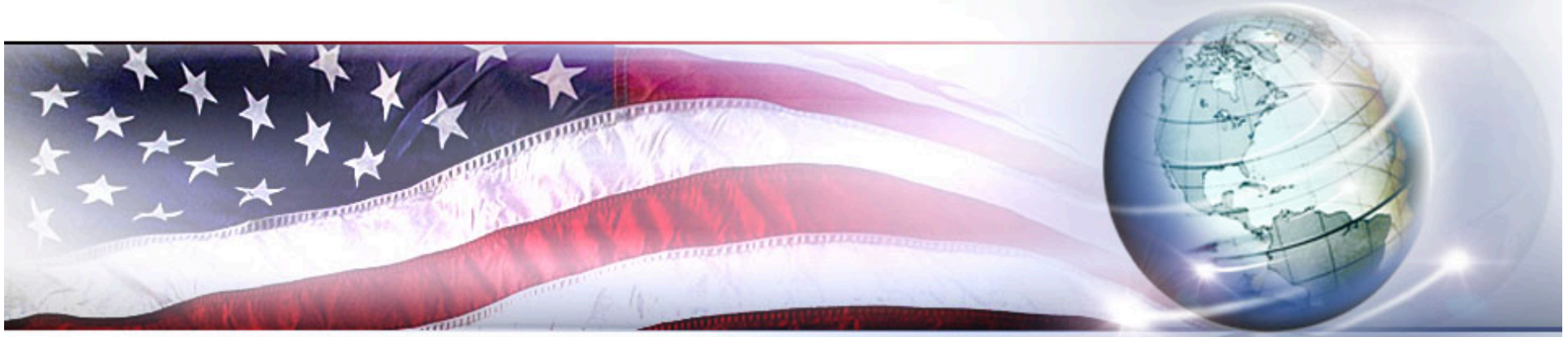
System and Software Assurance

GMU AFCEA Symposium – 2014



Brian Gallagher
Senior Vice President, Operational Excellence
May 20, 2014

INFORMATION DEPLOYED. SOLUTIONS ADVANCED. MISSIONS ACCOMPLISHED.

CACI
EVER VIGILANT

Operational resilience

- **Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]**
- **Operational resilience: The emergent property of an organization exhibited when it continues to carry out its mission after disruption that does not push it beyond its operational limit [CERT®-RMM]**
- **Resilience is an operational characteristic or quality attribute and is therefore a systems engineering design consideration.**

CACI
EVER VIGILANT

How do you Design a Resilient System?

- System Architectural Considerations: Redundancy, Separation of Concerns, Enclaves, Failover, Load Balancing, etc.
- Software Architectural Considerations: High reliability architectural patterns, Separation of Concerns, Fault Tolerant, etc.
- Software Implementation Considerations: Secure coding, "rugged" software, proof carrying code, etc.

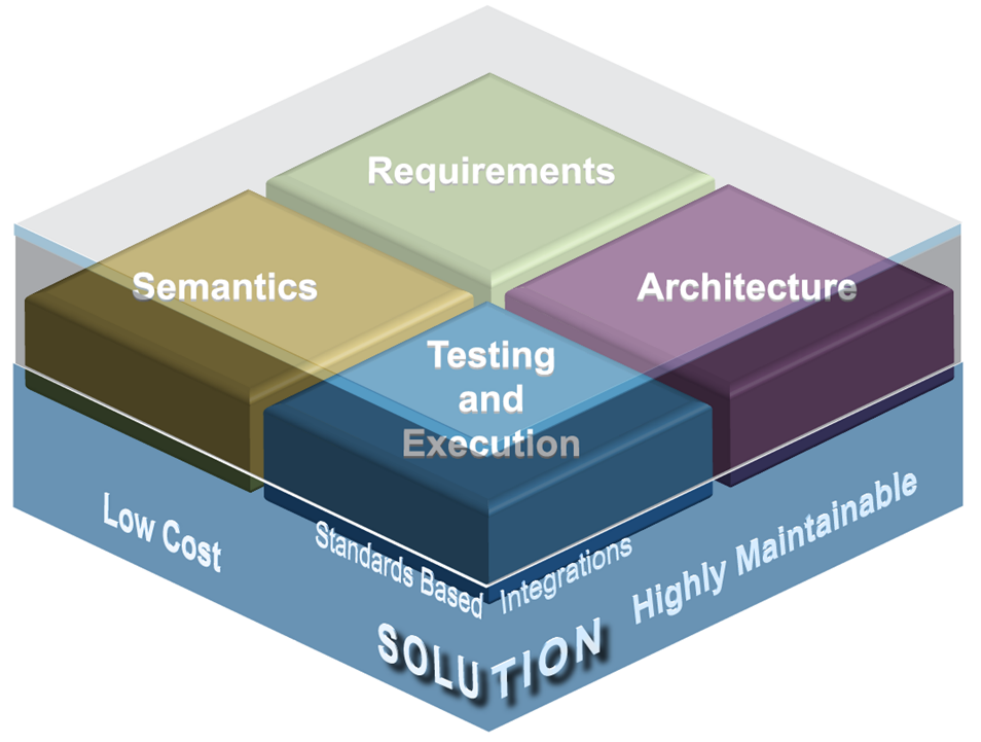
What does Resiliency have to do with Assurance?

- **You can't guarantee bad things won't happen**
- **You *can* decide the how you want the system to behave when bad things *do* happen**
- **Treating Resiliency as a system-level design consideration, or quality attribute, allows you to make informed design decisions that drive operational behavior**

CACI
EVER VIGILANT

Model-Driven Design and Implementation

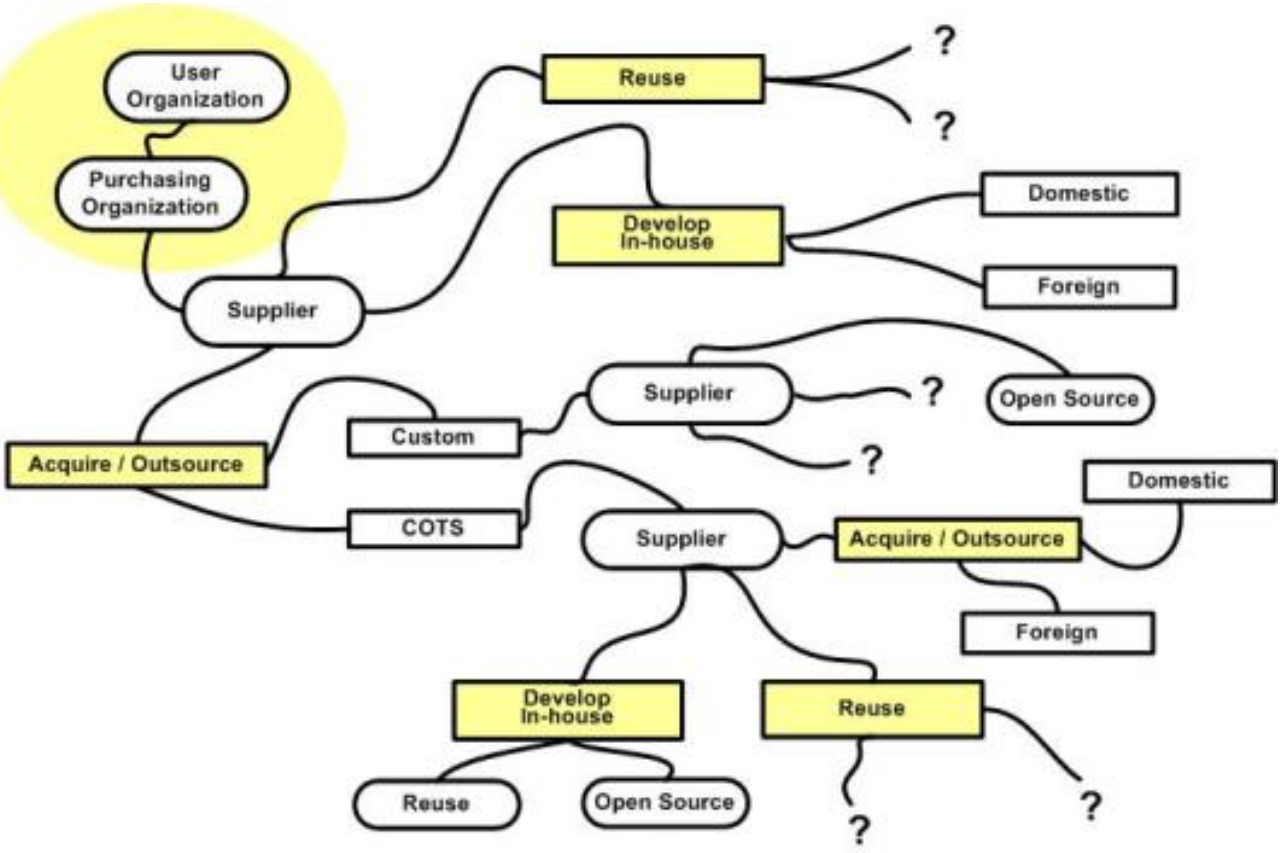
MDDI is an architecture-centric standards-based, repeatable methodology that accelerates the delivery of solutions satisfying our clients' most challenging problems by integrating *business and mission objectives, requirements, architecture, design, testing, semantics, and executable code in a shared model allowing client visibility and development agility.**



** resiliency, redundancy, interoperability, reliability, modifiability, etc.*

CACI
EVER VIGILANT

Complexities of Supplier Assurance



Potential Software Supply Chain Paths

[https://buildsecurityin.us-cert.gov/swa/forums-and-working-groups/acquisition-and-outsourcing]

CACI
EVER VIGILANT

Controls: Secure Supply Chain Management

ISO 28000/ISO 27001/CERT-RMM/NIST Cyber Security

Founded on Threat Management Delivering Supply Chain Resilience

Identification-Prevention-Detection-Response-Recovery

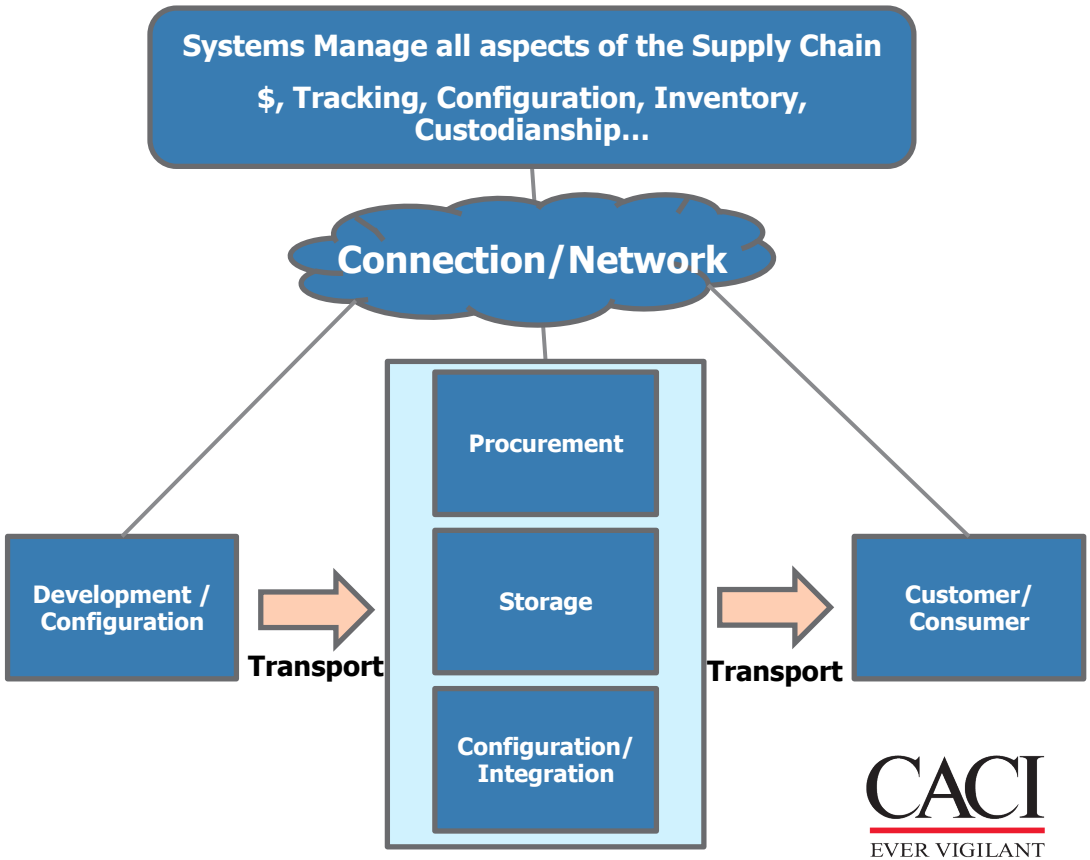
Threats/ Attacking Agents

- Counterfeit Parts
- Collusion
- Fraud
- Espionage
- Environment
- Nature
- Thief
- Piracy
- Spillage
- Terrorism
- Contamination
- Sabotage (Open Source Code)
- Viruses/ Malware
- Insider Threat

Security Controls

- InfoSec
- Supplier Management
- Compliance
- GPS Carrier Tracking
- Counterfeit ID Program
- Malware Detection
- Operations Security
- Incident Mgmt
- Access Control
- Asset Mgmt
- Environment Security
- Physical Security
- Hazmat Program
- HR Mgmt
- Training Program(s)
- Preparedness Testing

Supply Chain Management



CACI
EVER VIGILANT

Questions?

CACI
EVER VIGILANT