Software Assurance v. Security Compliance: Why is compliance not enough?

Carol Woody, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Acquisition & Development Landscape

Material Solution Analysis
Material Development Decision

Pre-Systems Acquisition

Technology Development

Systems Acquisition

Engineering and Manufacturing Development
Post-CDR A

Production and Deployment
FRP Decision Review

Sustainment

Operations and Support

Certification and Authorization to Operate

Security Controls Established

Software Supply Chain

Software Patch Cycle

Program Office
Prime Contractor
Supplier
Acquire
Acquire COTS
Develop In-House
Outsource
Develop Offshore
US Developers
Foreign Developers

Contractor

Reuse
Develop In-House
US Developers
Foreign Developers

Develop in US

CERT
Software Engineering Institute | Carnegie Mellon
Security Compliance

- Manage risks related to the use, processing, storage, and transmission of data.
- Enforce security policies; control and audit access.
- Protect data; encrypt communications and data stores.

From TACP-M VCS TRD dated January 2008
How is Security Compliance Addressed?

Effective **system** engineering is considered sufficient to address security

Security requirements are:

1. Established at the system level and described as confidentiality, integrity, and availability (CIA) controls
   - DoD policy based on mission assurance category (MAC) per DoD 8500.2
2. Assigned to components through system engineering decomposition
3. Not required until Milestone B
(1) What Security Controls Don’t Address

Software weakness: poor handing of unexpected conditions such as not rejecting invalid input

Design weakness: unanticipated consequences (example on next slide)

Becomes a vulnerability when an attacker can create conditions that leads to adverse behavior.

- Installs a malicious program
- Accesses or changes protected data
- Create unexpected system behavior
(1) Design Weakness: Unanticipated Response

Threat
If a malicious attacker gains control of an UAV

Consequence
Then the UAV could be used to attack US forces

Attack Steps
1. Encrypted GPS signal is jammed.
2. Navigation system fails over to an unencrypted civil GPS.
3. Authentic GPS signal is overpowered.
4. UAV is under the control of a malicious attacker.

M1: Include a redundant navigation system that is not reliant on GPS

M2: Ensure that navigation system does not fail over to an unencrypted civil GPS when jammed

Possible GPS Spoofing of a UAV (see slide 30 for references)
(2) Systems Engineering – Components

Systems Engineering Assumptions

- Systems can be decomposed into discrete, independent, and hierarchically-related components (or subsystems).
- **Is part of:** Components can be constructed and integrated with minimal effort based on the original decomposition.
- Security properties can be allocated to specific components.

Software Engineering Realities

- Software components are often related sets of layered functionality (one layer is *not* contained inside another layer).
- **Is used by:** Interactions of the components (*not* the decomposition) must be managed.
- Security properties relate to composite interactions (*not* to individual components).
(2) Role of Software in Systems

Independence of Software Components is Uncertain
Growing use of software increases risk of a false assumption

From the *NRC Critical Code Report, p.19*

“Software has become essential to all aspects of military system capabilities and operations”

1960 – 8% of the F-4 aircraft functionality
1982 – 45% of the F16 aircraft functionality
2000 – 80% of the F-22 aircraft functionality

(2) Systems Are Highly Interconnected

What is the System? Where is the Software?

- Processing Environment
- Data Storage
- Data Retrieval
(3) Acquisition Before Milestone B

Security Controls Established

Certification and Authorization to Operate

Pre-Systems Acquisition

Material Solution Analysis
Material Development Decision

Technology Development

Engineering and Manufacturing Development
Post-CDR A

Production and Deployment
FRP Decision Review

Systems Acquisition

Sustainment

Operations and Support

Request for Proposal
Contract
Component Selection

Software Supply Chain

Contracts do not include consideration for software and design weaknesses
(3) Supply Chain Participants

**Acquirer**
- Product acquisition
- System/service acquisition

**Supplier**
- Prime contractor
- Sub-contractors

**Attacker**
- Target of opportunity
- Focused targeting
(3) Views and Priorities Vary Widely

**Attacker**
- Incentives & enablers
- Value of data or service
- Exploitable defects & features

**Product Impact**

**Supplier**
- Sub-contractor
- Supply chain
- Risk-based development
- Governance

**Operational Impact**

**Acquirer**
- Feasibility: what can be controlled
- Business Risks
- Possible tradeoffs
  - acceptable risks
  - expense
  - functionality
  - network
  - connectivity
  - end-user access

**Contract Response**

**Buyer Options**
Security Compliance Limitations

Security compliance focuses on data protection - weaknesses in software and design can be missed.

System engineers focus on component properties and can miss software security requirements important to the composition (components interacting).

Many acquisition decisions affecting software security are made before Milestone B.
Software Realities

There is no such thing as perfect code.

- Best-in-class code contains 2.5 errors per function point.
- Average quality is 4.5 errors per function point.

There are too many possible combinations for code to be fully tested to confirm “functions as intended.”

The threat landscape is constantly changing.

- Evolving nature of threats, usage, and product functionality
- Skilled attackers that know system weaknesses better than defenders
Software Assurance (SwA)

Defined as “the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.” National Information Assurance Glossary; CNSS Instruction No. 4009

Focus on:

Software assurance is a level of confidence for

- **Trustworthiness** - No exploitable vulnerabilities exist, either maliciously or unintentionally inserted.
- **Predictable Execution** - When executed, software functions as intended.
Mission Success requires acceptable software behavior over a spectrum of operational conditions, including attacker-created events. Software Assurance methods support this objective.
Software Assurance Focus

An attacker uses weaknesses in the functional code to go around security controls.

Attackers gain access by creating failure conditions that are not properly addressed by the software design and implementation.

Requirements must represent how the system will “function as intended” under all operational conditions.

System operational behavior can be characterized by operational mission threads (extending use and abuse cases to the operational mission level).
Mission Thread Analysis: Process to Characterize Operational Behavior for Software Assurance
Mission Thread Analysis

Focus on the **successful** completion of a mission (i.e., satisfactory execution of each critical step)

Analysis Framework Process

1. Assemble critical operational mission threads
2. Define critical mission steps and successful completion (sequenced activities, participants, and resources)
3. Define ways that execution can be compromised at each critical step (execution failure, threats of attack, etc.).
4. Evaluate the effectiveness of existing requirements for response and recovery.
5. Update requirements to address unacceptable risk
Explore Mission Failure Issues

What errors could occur and how would that impact the mission?

Who identifies and manages the error?

- Coordination of responses across multiple systems—how do you do concurrent end-to-end management (possibly multiple contractors)?

Which faults should be visible to a user?

- Fault reporting can easily overload resources (especially mobile devices).
- Will the user understand an error and know what to do?
Example: Close Air Support Mission Thread (CAS)

1. CAS request to Army command
2. Army communicates CAS request to JTAC
3. JTAC submits request which is reviewed and approved/disapproved by ASOC
4. Aircraft transits to control point; ASOC passes control to JTAC
   JATAC updates Air Tasking Order (ATO)
5. Target attacked
6. Egress
7. BDA status communication to Command & Control

Air Support Operations Center (ASOC)

Arrives on Station

Plane Tasked

Head Quarters

Battalion Head Quarters

JTAC
CAS: Communication Is a Source of Failures

Strategic: Web-based Clients

Operational: Mix of clients types

Tactical: LOS, Thick clients, capable of operating with GIG access, with ad-hoc, peer-to-peer, or with no network.
Communication Is a Source of Failures

For tactical wireless networks, management of adverse communications can involve application software and network management. For example, during low bandwidth conditions, tactical mission software could reduce network requests and synchronize only critical data among units.

Tactical: LOS, Thick clients, capable of operating with GIG access, with ad-hoc, peer-to-peer, or with no network.
Mission Step Failure Analysis

Evaluate coordination across multiple systems

Can the system adapt if not all expected conditions are met?

People Involved

Mission Step
- Sources for failures
- Mission impact
- Recovery options

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Manual Intervention

Next Step

Automatic

Resources Required

Man
Mission Thread Analysis Results

- Connects technology and mission success
- Provides visibility for actions across systems that are independently designed and developed
- Supports failure analysis and mission impact of failure
- Identifies gaps in system requirements
- Builds the case for system assurance - justified confidence of the delivered system
Summary

Software is everywhere and all software has vulnerabilities

Focusing on technical security compliance for a system is necessary but not sufficient – everything is interconnected

Risk management is critical and people (acquirers, designers, coders, and users) are part of the risk

Software assurance requires consideration of the mission impact of security failure
Mission Thread Analysis Resources

*Survivability Analysis Framework*, Robert Ellison and Carol Woody. 
http://www.sei.cmu.edu/library/abstracts/reports/10tn013.cfm

References: GPS Spoofing of UAV

Media reports – Lockheed Martin RQ-170 Incident


Humphreys, Todd. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing.*

Contact Information

Carol Woody
(412) 268-9137
cwoody@cert.org

Web Resources (CERT/SEI)
http://www.cert.org/
http://www.sei.cmu.edu/
Acronyms

ASOC – Air Support Operations Center
ATO – air task order
BDA – battle damage assessment
JTAC – joint tactical air controller