Vulnerability Assessment in Test Plan Design Verification

NASA IV&V Annual Workshop
University of West Virginia

Fairmont, VA
September 13, 2011

Outline

- Vulnerability, risk, and treat – Definitions
- Current IV&V of test plan: advantages and disadvantages
- Components of System Vulnerability Defined
- A Vulnerability Approach for tests' IV&V
- IV&V Analysis Phases
- Analysis Examples
- Future Plans and Conclusions

Vulnerability- NIST definition

NIST SP 800-30 – Risk Management Guide for Information Technology Systems:

- Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability- ITSEC definition

The Information Technology Security Evaluation Criteria (ITSEC is used by a number of European Countries), vulnerability definition is more general:

- Vulnerability: The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

Vulnerability – Associated Terms

1. The **susceptibility** of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.
2. The characteristics of a system that cause it **to suffer** a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.
3. In information operations, a **weakness** in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.

Dictionary of Military and Associated Terms. US Department of Defense 2005.

Definitions of Risks

- ISO Guide 73 – Risk Management defines “risk” as: The combination of the ***probability*** of an event and its consequence
- ISO 13335 – Information Technology Security Techniques defines “risk” as: ***The potential that a given threat*** will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

So we can interpret risk as probability of a treat to negatively affect a system because of a specific design limit. This design limit defines the vulnerability of the system to exhibit degraded performance when exposed to a treat

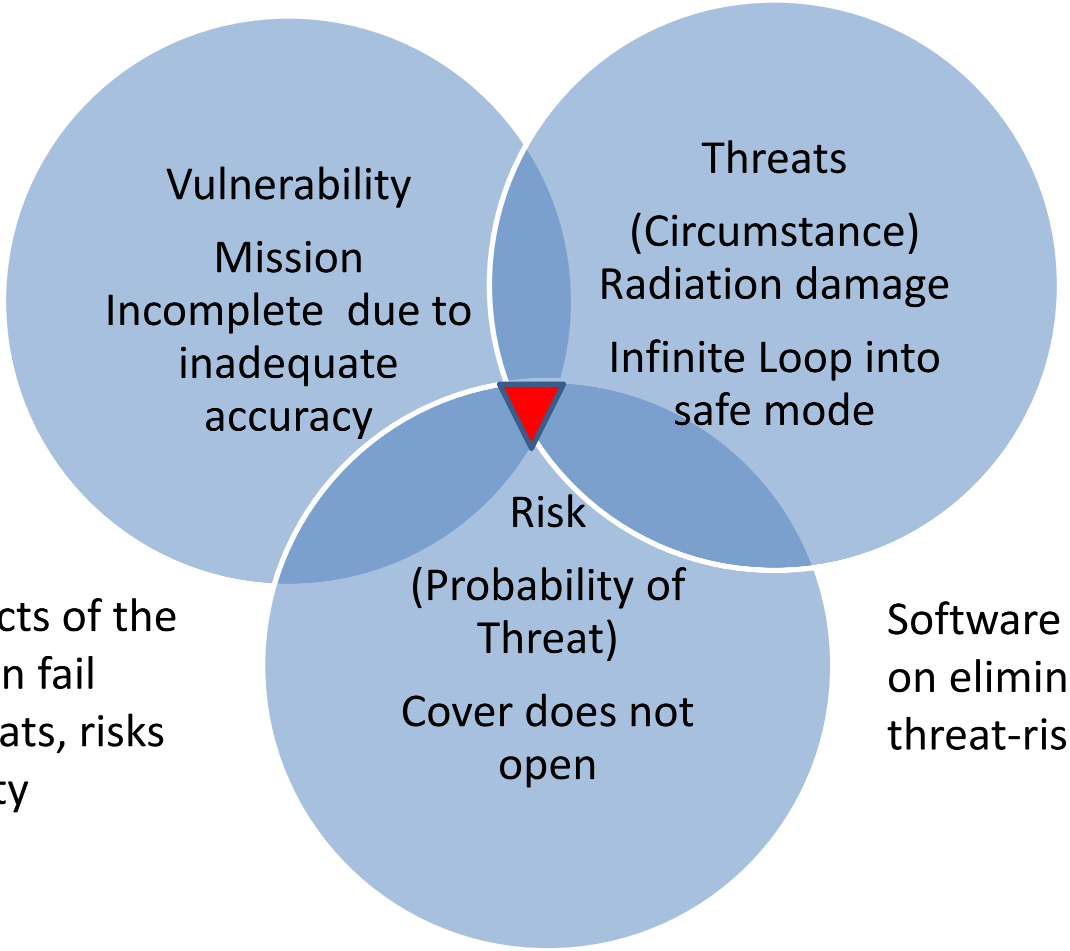
http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/

Definitions of Threat

- Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

- Both, NIST SP800-30 and the Common Criteria for ITSE (ISO standard replacing ITSEC) differentiate between a “threat source” or “threat-agent” and a “threat”.

Vulnerability


Vulnerability
Mission Incomplete due to inadequate accuracy
Threats
(Circumstance) Radiation damage
Infinite Loop into safe mode
Risk
(Probability of Threat)
Cover does not open

Individual aspects of the mission plan can fail only when threats, risks and vulnerability overlap.

Software IV&V focuses on eliminating any threat-risk overlap.

Vulnerability (cont.)

“Vulnerabilities are the gateways by which threats are manifested” (SANS)

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. It analyzes the major services in a system design to categorize risks in the Project Plan according to the three components or dimensions of vulnerability:

- Sensitivity
- Exposure
- Adaptive capacity, in the case of flight SW is Fault Protection (FP)

Current Test Plans Advantages

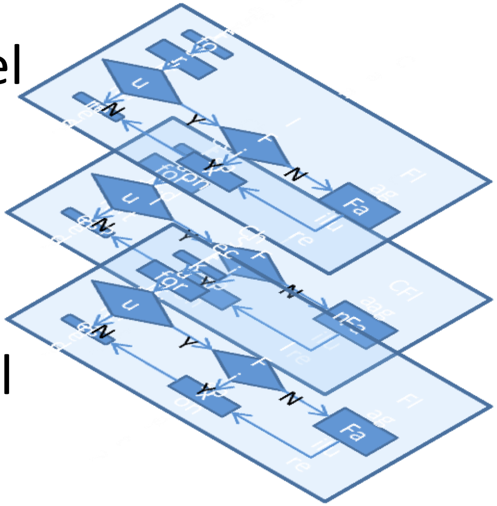
- As complete as the RTM
- Establish a detailed map of FSW performance parameters and functionalities according to design structure (white box test)
- Straightforward planning of regression testing in case of updates
- Well defined test verification process

Current Test Plans – Disadvantages

- Limited to the completeness of the RTM
- Assumes that all missing requirements were identified
- Assumes that all possible mission needs and system constraints
  - are captured in the SW system requirements (Q1, Q2 & Q3)
  - are properly propagated between HW and SW interfaces (Q2 & Q3)

Layered FP and Adaptive Capacity

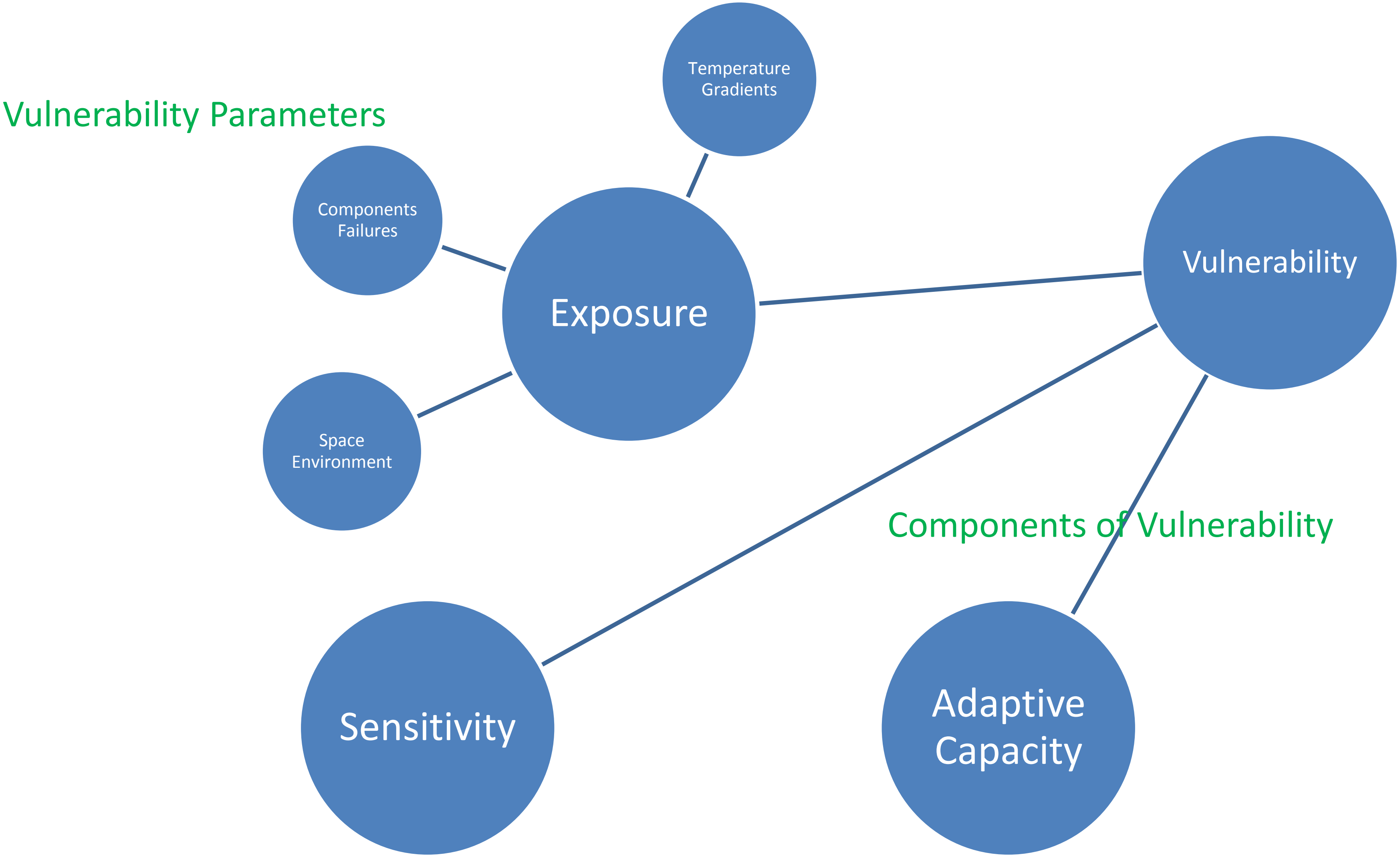
- Action list for System Level Faults
- Action List for Unit & System Performance Level Faults
- Action list for Component-Network Level Faults



Question: Are all the actions be safely implemented during all:

- phases of the mission?
- measurements routines?
- Maneuvers?

Components of Vulnerability: an Approach



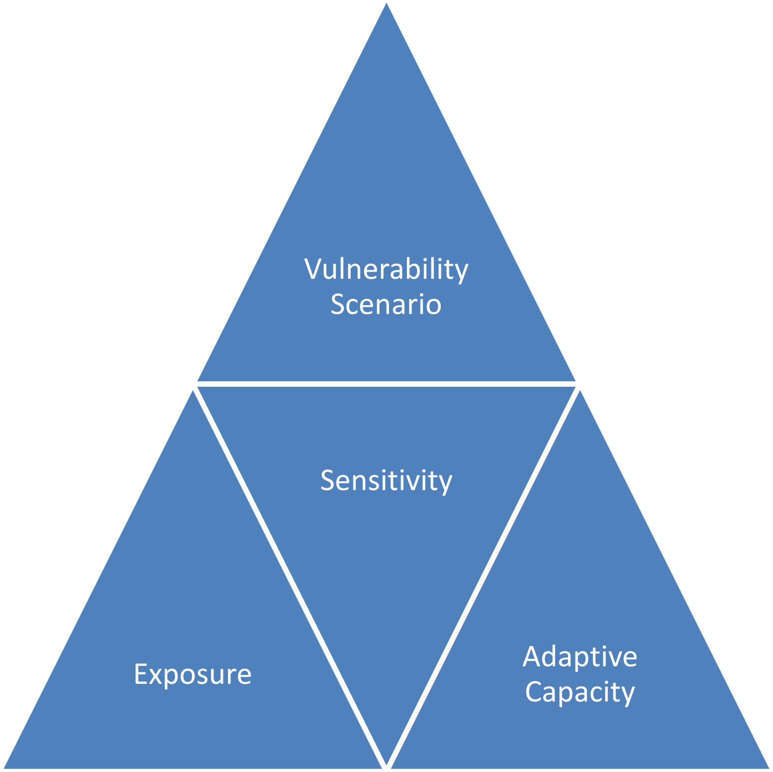
Vulnerability based test analysis

- Prioritizes vulnerabilities on the basis of CDR design
- Addresses critical issues that might be hard or costly to remediate
- Focuses on functionalities across code segments
- Identifies vulnerabilities across communication lines and HW –SW interfaces
- Provides criteria for building vulnerability scenarios to use during IV&V test plans analysis

Vulnerability Analysis Phases

- From Project Plan at PDR and CDR, list each type of vulnerability (sensitivity, exposure, adaptive capacity)
- Prioritize vulnerabilities according to severity and risks perhaps based on Portfolio Based Risk Assessment (PBRA) light
- Develop SOA diagrams as needed (Use Case Analysis, Activity Diagrams, Sequence Diagrams, etc.)
- Create black-box tests
- Trace vulnerabilities through low level requirements
- Trace functionalities in test cases to black-box tests procedures

Vulnerability Assessment Protocol



The Issues	*The Decision Making Approach*
Vulnerability assessments goals: *help potentially vulnerable entities identify ways to protect themselves and their resources by assessing their:*	**Severity Priority Levels, Risk & Likelihood of occurrence, Solutions, and cost estimates**
Sensitivity: *The degree to which systems and subsystems can be harmed by a hazard (or attack).*	**Severity of Problem, adequacy of the systems for the mission (TRL)**.
Exposure: *The likelihood and severity of possible hazards.*	**Hazards (Distribution and Severity) possible** causes of disruption of service.
Adaptive Capacity: *How system design can (FP) can mitigate the risks posed by their exposure and sensitivity.*	**Solutions and mitigation** approaches feasible within a defined system.

Threats & risk analysis

1. List the events (threats) that can occur during the various mission phases and that may negatively affect system performance (exposure)
2. Analyze the probability that any combination of threats may cause operating parameters to exceed thresholds during operations and transitions
3. Investigate viable remediation strategies
4. Evaluate possible effect on mission goals (vulnerability)
5. Apply results to IV&V test plans analysis

Vulnerability Test Plan V&V

Verify that test plans validates:

- Threshold parameters and functionalities related to the threads and risk analysis
- FP procedures that minimize off nominal operations for significant vulnerabilities
- Document potential issues arising from erroneous propagation of corrective actions into other segments of the system (e.g. ground operations)

Conclusions

Vulnerability analysis:

1. Saves on resources because it specifically address:
   - Risks with potentially significant impact on a mission
   - Facilitates tracing risks across services by creating the diagrams needed for risk analysis
2. Improves on present practice of test plan analysis by:
   - Considering occurrence of combination of adverse events (e.g. memory radiation damage occurring during software upload)
   - Addressing requirements and test plan potential issues early in the design phases
3. Directly applies other previous missions "Lesson learned" to designing adverse scenarios
4. Verifies system compliance to the three questions across interfaces and multiple mission phases

Future Work

Future Work

1. Pilot study can be conducted on a small test system with:
   - Multiple services
   - Complex scheduling of services
   - Several interfaces and mission phases
2. Application to a larger scale aerospace system