



**Carnegie Mellon
Software Engineering Institute**

Pittsburgh, PA 15213-3890

Diagnostic Software

What your Developer Doesn't Know

Ted Marz

tfm@sei.cmu.edu

A presentation of paper CMU/SEI-2005-TN-035
Integrated Diagnostics: Operational Missions, Diagnostic Types, Characteristics,
and Capability Gaps
<http://www.sei.cmu.edu/publications/documents/05.reports/05tn035.html>

Sponsored by the U.S. Department of Defense
© 2005 by Carnegie Mellon University

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JAN 2005		2. REPORT TYPE		3. DATES COVERED 00-00-2005 to 00-00-2005	
4. TITLE AND SUBTITLE Diagnostic Software What your Developer Doesn't Know				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 13	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Motivation

- Involved in several software intensive systems development activities
- Observed a lack of operational knowledge on diagnostics in the system development teams
- Lack of knowledge in non-traditional developments
- Near total lack of integration between O-Level and I-/D-Level diagnostic and repair activities
- Seen how diagnostics can impact Life Cycle Cost
 - Increased Spares
 - CND / RTOK rates in the repair process
 - Manning / Staffing issues of operational systems



Diagnostic Software

The DoD is dependent on increasingly complex, software intensive, hardware/software hybrid systems to achieve their mission.

Assurance of mission capability is a primary operational need.

- Fault Detection (FD) supports that need
- Fault Isolation (FI) assists in assessing the impact of a failure

Diagnostic capabilities are a co-development problem.

Lack of effective FD/FI and Restoration practices impact system lifecycle cost in multi-dimensional ways.

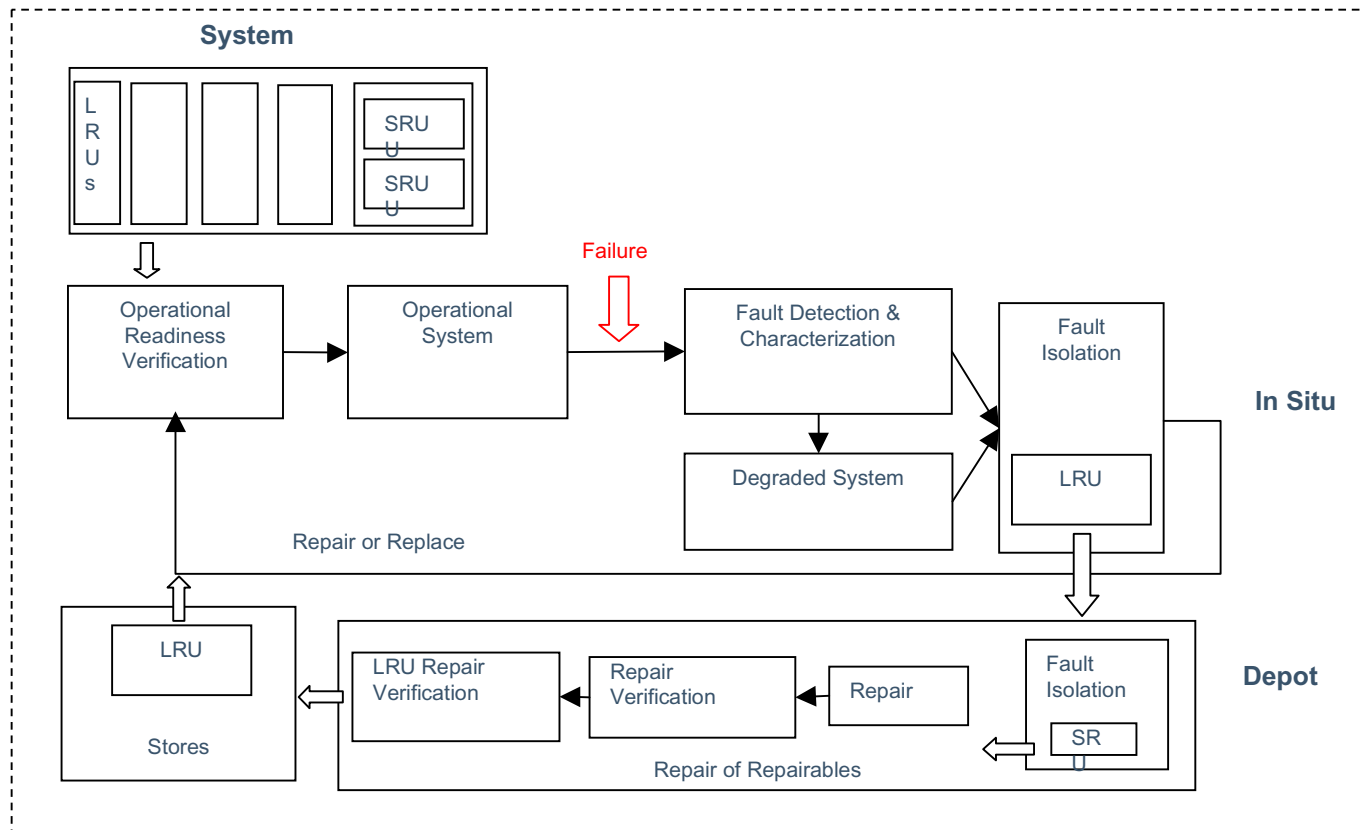
FD/FI capabilities are not generally considered core requirements by the developers.



Diagnostic Operational Missions

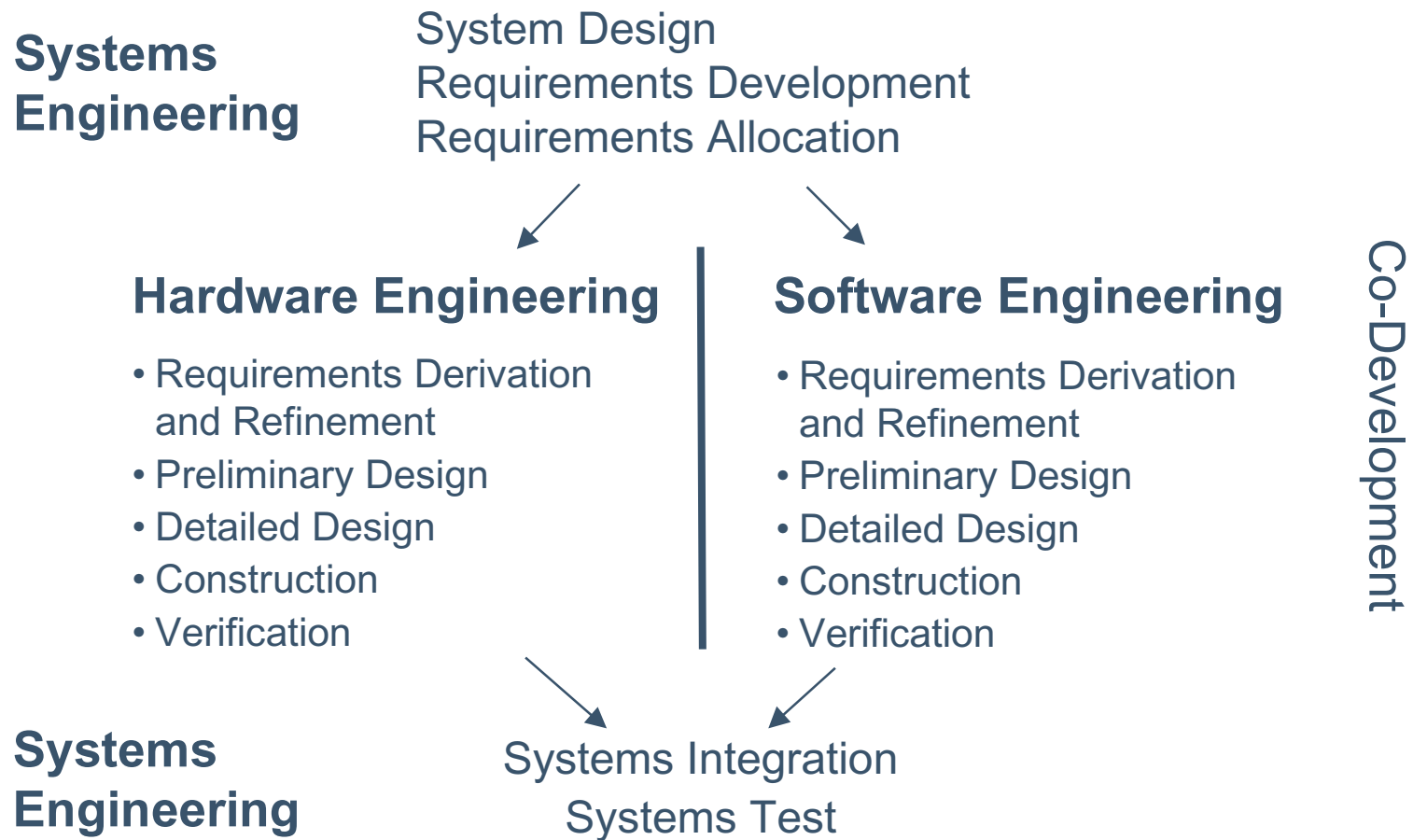
- Verification of Operational Readiness
Am I Mission Capable?
- Fault Detection (FD) and Characterization
Have I failed mid-mission?
What are the effects of failure? Can I continue?
- Fault Isolation (FI)
What has failed? What do I need to replace?
- Diagnosis and Repair of Repairables
FI at the lower component level; Repair verification
- Other Maintenance Actions
Installation, Configuration, Alignment, Calibration, etc.

Logistics Support Cycle



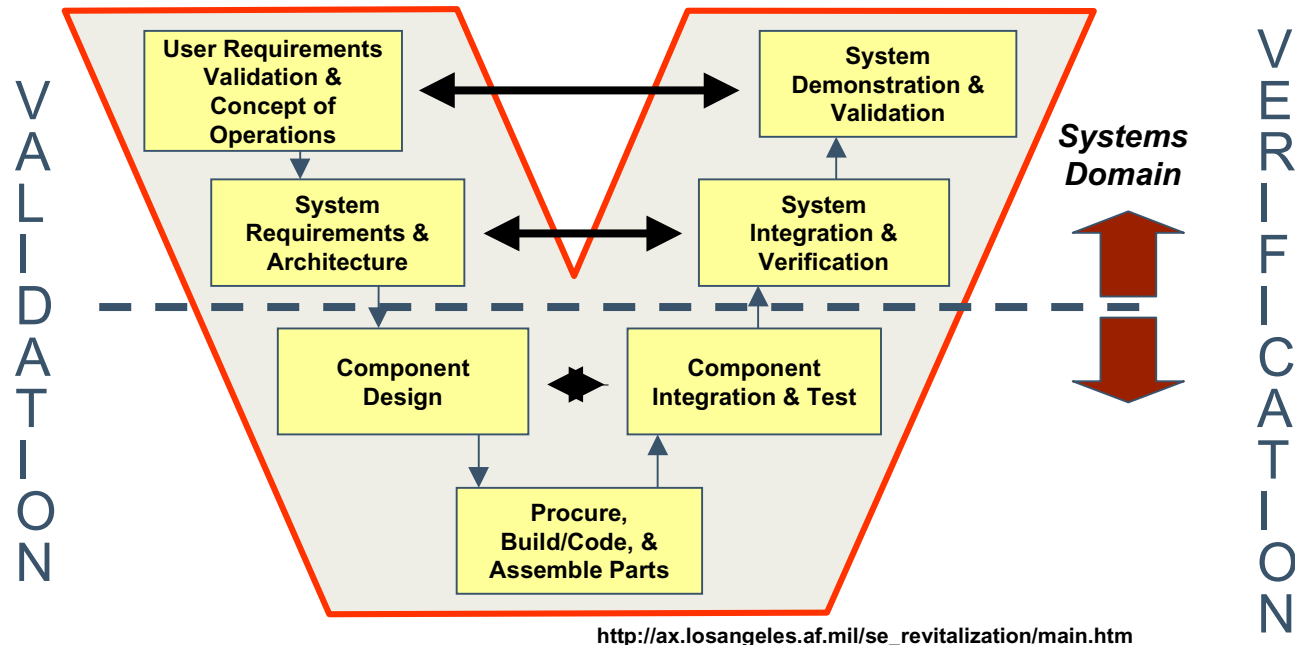


System Development Process





System Validation Activities



- Engineering Reviews at all levels are Validation events
- Acquisition Program Office MUST participate in validation events.
 - Balanced with other responsibilities
 - Resourced with appropriate capability



System Safety influence diagnostic maturity

Safety is a prime driver, as it is a major concern of the verification and validation efforts.

Domains with strong safety concerns exhibit more mature diagnostic environments

- Regulatory & Liability responsibilities drive activities
- System Safety Engineering Program
 - Failure Modes, Effects & Criticality
 - Undiagnosed failures lead to unsafe conditions
 - Recognized software safety standards applied

Example Domains

- Avionics & Flight controls
- Nuclear & other Power Generation
- Chemical Process Control
- Medical Instrumentation & Devices
- Telecom



Even Mature Environments Fail

Example – recent F-22 flight controls related crash.

Non-Traditional Environments Fail Spectacularly

Example – mission critical IT system

No verification of operational readiness

No online fault detection / isolation

Internet hosting service not doing system performance monitoring



Hardware BIT is not sufficient

Diagnostics is an Operational Mission need

- Verify capability wherever it is implemented
 - Distributed, “Net Centric” & SOA systems
 - Programmable Hardware environments (FPGA, etc.)
 - Software implemented capabilities
- Software component health has not been a significant concern to date
 - Ad Hoc methods
 - Spotty coverage
 - Inconsistent handling & reporting
- Software health reporting should be part of the overall systems health management environment



What Developers Should Do

- Consider the Integrated Diagnostics and other System Sustainment and Support capabilities part of the core mission
- Explicitly treat Integrated Diagnostics as a co-development problem, with appropriate, multi-disciplinary Integrated Product Team support
- Fold software health management into the overall system health management environment
- Better consider integration of the in-situ and Depot diagnostics environments



What Program Offices Should Do

- Better integrate logistics support (diagnostics, test, maintenance, repair) in the development activities currently supported by the Hardware and Software validation teams
- Resource the validation teams to better support the acquisition effort
 - Be prepared to augment the developer with operations expertise from similar, legacy systems
- Create realistic diagnostic coverage requirements
- Better define the needs of the on-line and off-line diagnostics environments
- Create requirements for the integration of the in-situ and Depot maintenance environments

Contact Information

Ted Marz tfm@sei.cmu.edu