Software Verification and Reliability - II

Software Reliability Engineered Testing

"The *bitterness* of poor quality remains long after the *sweetness* of meeting the schedule has been forgotten."

--Anonymous

Review of yesterday's talk

- *Software Reliability* corresponds to *functional requirements* as well
  - Behavior of the system is the key
- *Cost* is a major barrier in terms of achieving high *Software Quality* and *Reliability*
- *Automation* is a long term investment, with potentially high returns
- *Formal methods* (or pseudo-formal methods) are not only good for *correctness*, they may also aid in *automation*

What is SRET?

- *Software Reliability Engineered Testing* (SRET)
  - An engineered *Test Process* that utilizes *Quantitative Planning* and *Tracking*
  - Considers *Reliability Objectives* and *Operational Profiles*
  - Devised at *AT&T Bell Labs* during the early 90s
  - Major contributor: *John D. Musa* (one of the creators of the field of *Software Reliability Engineering* (SRE))
  - **Reference:** Musa, J.D. "Software-Reliability-Engineered Testing". *IEEE Computer*, Vol. 29, Issue 11, pp.61-68. (1996).

Preliminaries

- Failure
  - "the departure of program behavior during execution from user requirements" … a *user–oriented* concept
- Fault
  - "the defect in the program that causes the failure when executed" … a developer–oriented concept
- Software Reliability
  - "The probability of execution without failure for some specified interval, called *mission time*."
- Types of testing SRET can be applied to
  - Feature (function), Load, Regression, Certification, Acceptance

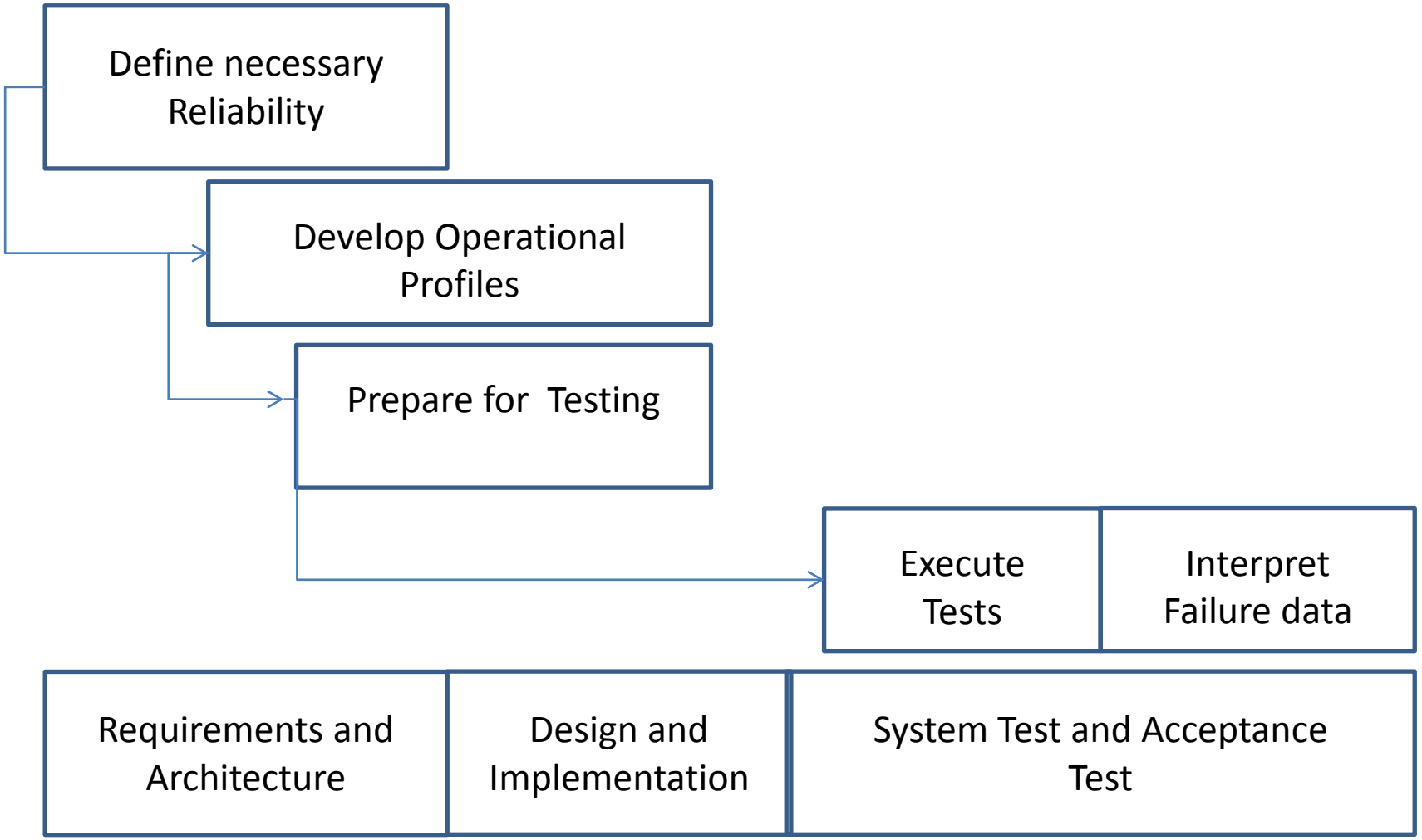
Preliminaries … contd.

- Execution time
  - “actual time used by the processor in executing a program’s instructions”
- Failure Intensity
  - “failure per unit execution time”
- Operational Mode
  - “a distinct pattern of system use and/or environment that needs separate testing because it is likely to stimulate different failures”
- Operation Profile
  - “set of operations and their probabilities of occurrence”
- Severity Class
  - “a set of failures that affect users to the same degree”

SRET – The phases

- Definition of *necessary reliability*
  - Determine *Operational Modes*
  - Define *Failure* in terms of *Severity Classes*
  - Set *Failure Intensity Objectives* (FIO)
  - Engineer *Reliability Strategies*
- Develop *Operational Profiles*
- Prepare for *Testing*
  - Specify *Test Cases*
  - Define *Test Procedure*
  - Execute Tests
- Interpret *Failure Data*

SRET – The phases … contd.



Example: *Fone Follower*

- A system that lets telephone calls follow users anywhere in the world
  - Users dial into a voice response system and enter the numbers at which they plan to be at various times
  - Calls can be forwarded to fixed lines as well as cell phones
  - In case of *Call Forwarding No Reply* (*CFNR)*, calls are forwarded to a pager service
  - In case the pager service does not respond, calls are forwarded to voice mail
- So how do we apply *SRET* to the *Fone Follower* project?

Fone Follower
Defining necessary Reliability … (1)

- Operational Modes
  - *Definition review: "a distinct pattern of system use and/or environment that needs separate testing because it is likely to stimulate different failures"*
  - *Peak Hours:* Heavy incoming calls and entries traffic. No administration or audit functions permitted
  - *Prime Hours:* Average incoming calls and entries traffic. Administration functions permitted, but audit functions limited
  - *Off Hours:* Low incoming calls and entries traffic. Low administration traffic, extensive audit traffic

Fone Follower
Defining necessary Reliability … (2)

- Defining Failure in terms of Severity Classes
  - *Definition review: "a set of failures that affect users to the same degree"*
  - *Class 1:* Failure prevents calls from being forwarded
  - *Class 2:* Failure prevents phone number entries
  - *Class 3:* Failure makes system administration more difficult, although it remains possible through alternate means. E.g. UI doesn't work, but terminal does
  - Class 4: Failure affects an operation that is deferrable, such as preventive maintenance

Fone Follower
Defining necessary Reliability … (3)

- Set Failure Intensity Objectives (FIO)
  - *Definition review:* Failure Intensity = *"No. of failures per unit execution time"*
- FIO is derived from:
  - Specific user needs
  - Existing system reliability

Fone Follower
Defining necessary Reliability … (4)

- Engineer Reliability Strategies
  - Fault Prevention
  - Fault Removal
  - Fault Tolerance
  - *Objective: "… finding the right balance among them to achieve the failure intensity objective in the required time; at minimum cost"*

Fone Follower
Develop Operational Profiles … (1)

- Definition Review
  - *"set of operations and their probabilities of occurrence"*
- How?
  - Identify the initiator operation
  - List the operations
  - Determine the occurrence rate per clock hour of the operations
  - Determine the occurrence probabilities

Fone Follower
Develop Operational Profiles … (2)

Operation	Occurrence Probability
Process voice call, no pager, answer	0.21
Process voice call, pager, answer	0.19
Process fax call	0.17
Process voice call, pager, answer on page	0.13
Process voice call, no pager, no answer	0.10
Process voice call, pager, no answer on page	0.10
Enter forwardees	0.09
Audit section - phone number database	0.009
Add subscriber	0.0005
Delete subscriber	0.0005
Recover from hardware failure	0.000001
Total	1

John D Musa. "*More Reliable Software Faster and Cheaper - How Software Reliability Engineering Can Help Testers*"

Fone Follower
Prepare for Testing … (1)

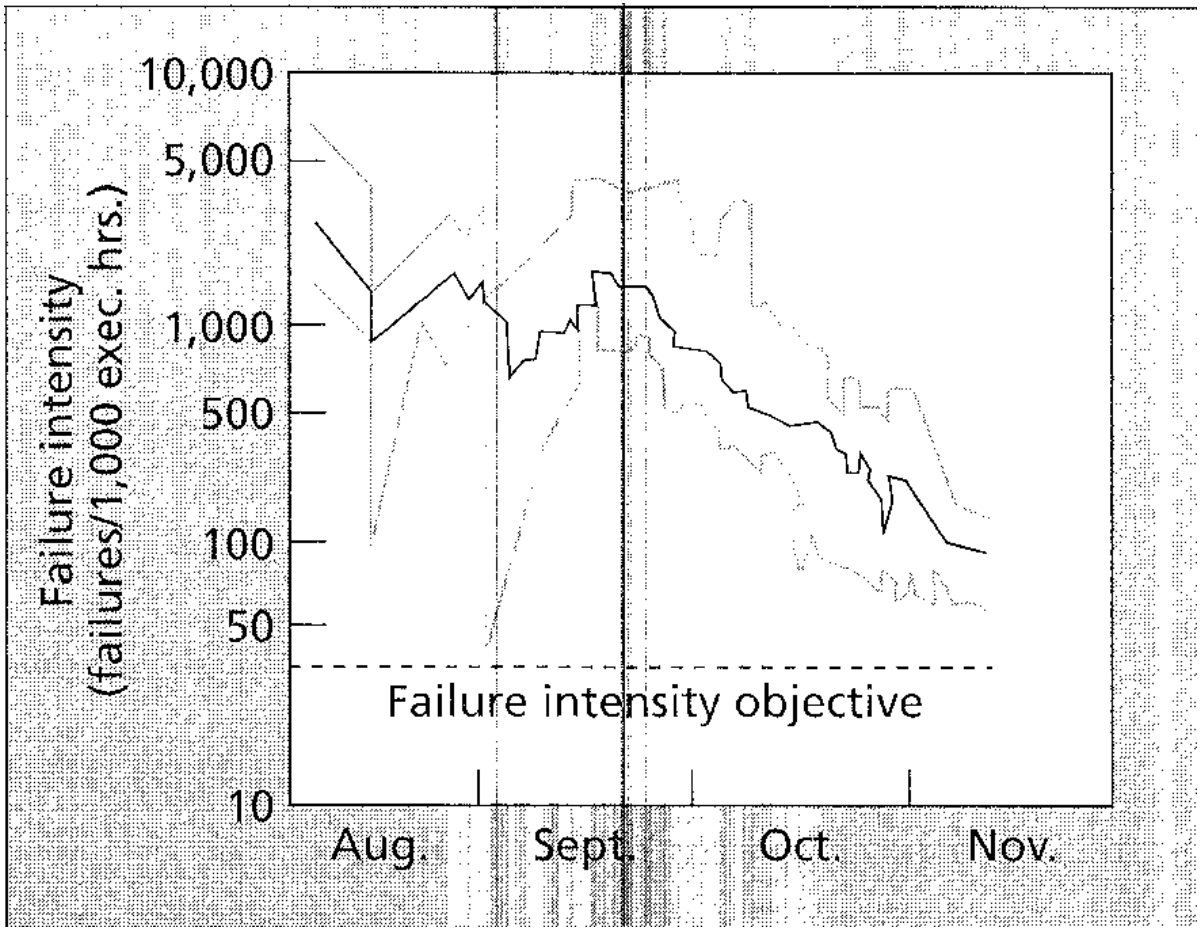
- Specify Test Cases
  - Select operations according to their *occurrence probabilities*
    - *E.g. for Fone Follower, since connect call has an occurrence probability of **0.71**, **71%** of TCs were for this operations*
  - *Definition: Level – "a value or a range of values of an input variable for which failure behavior is expected to be the same because of processing similarities"*
  - TC selection is done using *Levels*
- Why use *Levels*???

Fone Follower
Prepare for Testing … (2)

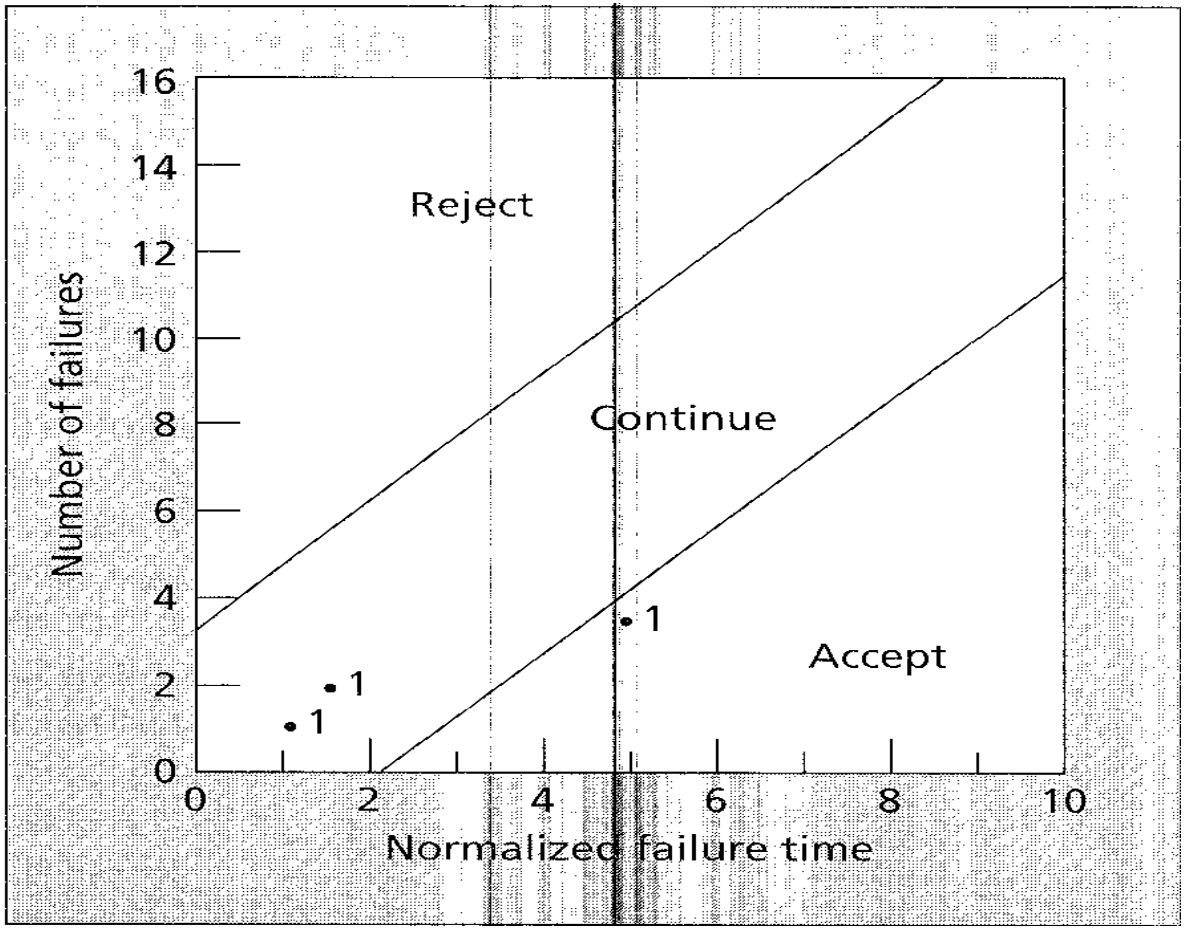
- Define Test Procedure
  - *Definition: "the specification of the set of runs and environment associated with an operational mode"*
  - A set of runs is specified statistically by using operation occurrence rates
  - Occurrence rates are used to select test cases randomly from the prepared set
  - Why use *Statistics* and *Randomization*???
- Execute Tests
  - *Feature Testing* is followed by *Load Testing*
  - *Operational Modes* dictate *Load Testing*

Fone Follower
Interpret Failure Data … (1)

- Consider Trends



Fone Follower
Interpret Failure Data … (1)



Reliability Demonstration Chart

Rview: SRET – The phases

- Definition of *necessary reliability*
  - Determine *Operational Modes*
  - Define *Failure* in terms of *Severity Classes*
  - Set *Failure Intensity Objectives* (FIO)
  - Engineer *Reliability Strategies*
- Develop *Operational Profiles*
- Prepare for *Testing*
  - Specify *Test Cases*
  - Define *Test Procedure*
  - Execute Tests
- Interpret *Failure Data*