"Software Systems Analysis Using Stress-Strength Probability Functions"

INCOSE 2011 International Conference

Jim Wilder
Boeing
June 2011

SW Reliability & Safety Characteristics

- IEEE Definition of Software Reliability:

"The probability that the software will not cause the failure of a product or of a mission for a specified time under specified conditions; this probability is a function of the inputs to and use of the product, as well as a function of the existence of faults in the software; the inputs to the product will determine whether an existing fault is encountered or not." – IEEE Std. Dictionary of Measures to Produce Reliable Software, ANSI/IEEE Std. 982.1

- Wearout and infant mortalities are not characteristics of SW failure, unless maintenance or updates introduce faults

- The definition indicates a reliability model should account for inputs to system and faults within system

- SW reliability characteristics:
  - a function of inputs to the software system, and the latent faults within the system
  - The probability of occurrence of specific modes is directly related to conditions which trigger those modes
  - The 'amount' of software – size – in execution varies with each mode

Safety Requirements

- Basic Goal of Safety:
  - Stable behavior around a known, safe operating state

- Customers often specify system safety requirement(s) as a probability of failure over time:
  - NASA – Space Station: "less than 1 in 1,000,000 possibility of loss of human life over 20 year operating life of Station"
  - Missile Defense Agency: "The probability of mixing of (simulated and real) data between sub-domains must be less than 10^{-6} over the life of the system."

- Complex systems and systems of systems can be thrown out of equilibrium by external, stressing conditions
  - Combinations of components may interact such that their combined effects are unstable or even unsafe

- Requirements and goal indicate a model that accounts for system behavior about a norm, with an associated probability.

- Definition indicates a SW model for safety that is function of (inputs, faults)
  - Both inputs and faults can be expressed as density probability functions for SW

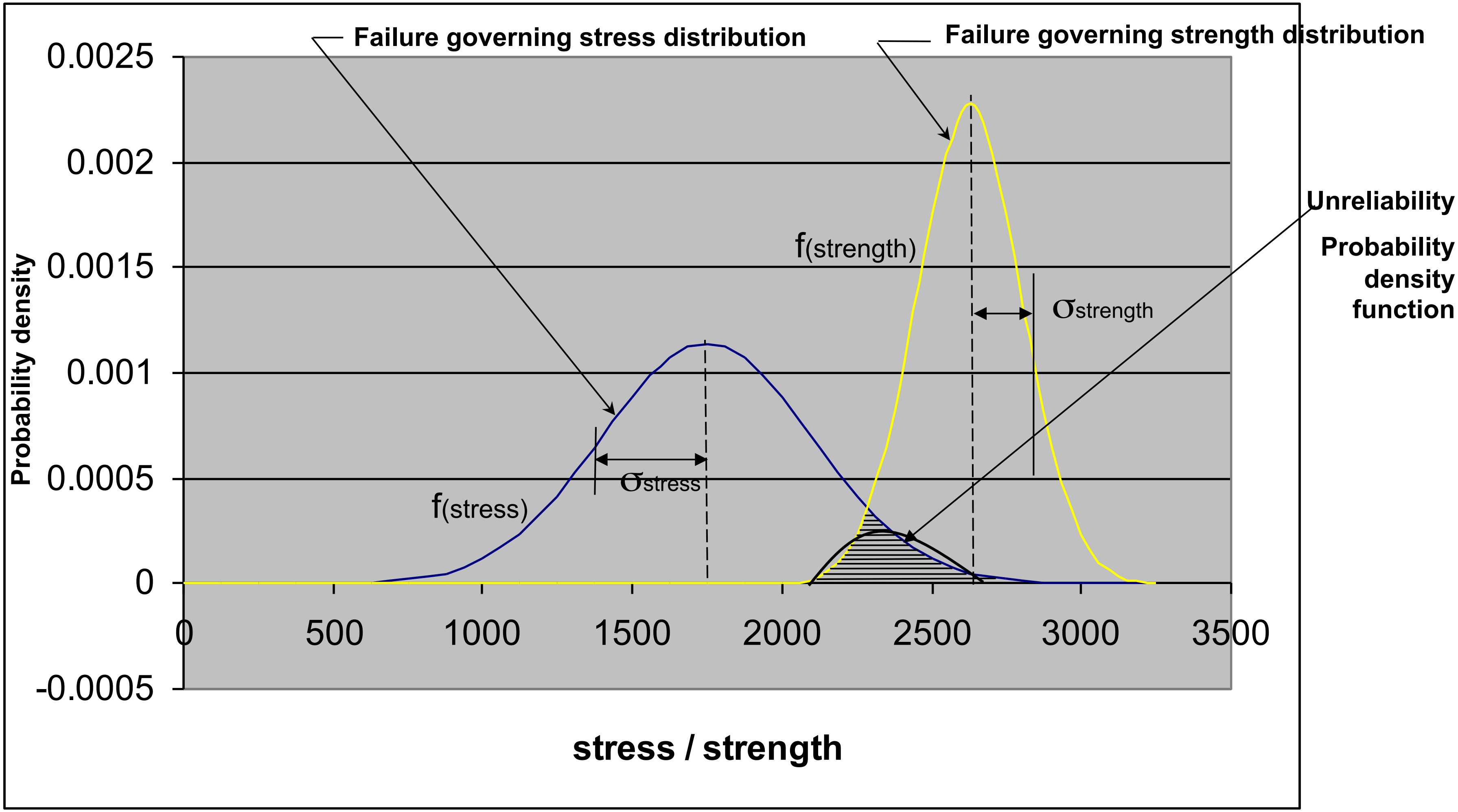
Theory of Failure

- Failure results when stress under the operating conditions exceeds the design-capabilities of the system.
  - Designate the designed capabilities of the system as ‘strength’
- The strength limit of the system can be described as the imposed stress level that induces failure.
- Fundamental Theory of Failure (usually applied to strength of material components):
  - “Identical components that have tolerances on their dimensions and are subjected to a range of loads during operation experience stresses that vary; thence the failure governing stress distribution.”
  - “Similarly, identical components that are made of materials which due to inhomogeneity, process variability, surface finish variability, etc. exhibit a range of strengths; hence the failure governing strength distribution. Coupling, mathematically, these two distributions yields the unreliability which is given by the shaded area in the figure.” (see next slide)
  - “This unreliability gives the designed-in probability of failure of such components, and the resulting failures would be classified as chance failures, if they are neither of the early nor of the wear-out type.”

Source: D. Kececioglu,1991: Prentice-Hall: Reliability Engineering Handbook, Vol. 1, pg. 74

The theory extends to general systems behavior, so long as strength and stress are defined in relationship to each other as probability functions.

Fundamental Theory of Failure



Failure governing stress and strength distributions with unreliability given by the shaded area

Predictions of System Safety

- The safety goal and prediction of system safety requirement is done by a statistical analysis of the stressing environment the system operates in, compared with the ability of the system to safely absorb the various stresses
  - Account for the operational environment

- This theory is applied to software behavior
  - In software systems, the well known concept of the “operational profile” can be used to define the stressing distribution
  - Systems strength is multi-variate function; several techniques, such as factor analysis or principle component analysis may be applied to consolidate and characterize strength from complexity metrics
    - Various complexity measures are weighted to determine the basic components of complexity
    - Complexity and stress distributions must be described with a common variate to apply this theory
    - The common dimension of “size” is applied in the example in the paper

This theory enables use of measures determined in the static domain (such as complexity and fault density) to be applied in dynamic, operating domains

Summary

- Overall behavior can be assessed as probability of resistance to failure (strength) and the stressing environment, if both are characterized by probability functions

- For systems dependent upon software, the operational failure rate is a function of the fault content of the software and the variability of software modes invoked by external conditions.

Development & Applications

- To develop and apply this theory requires the ‘strength’ of a system to be defined in terms of applied stress.

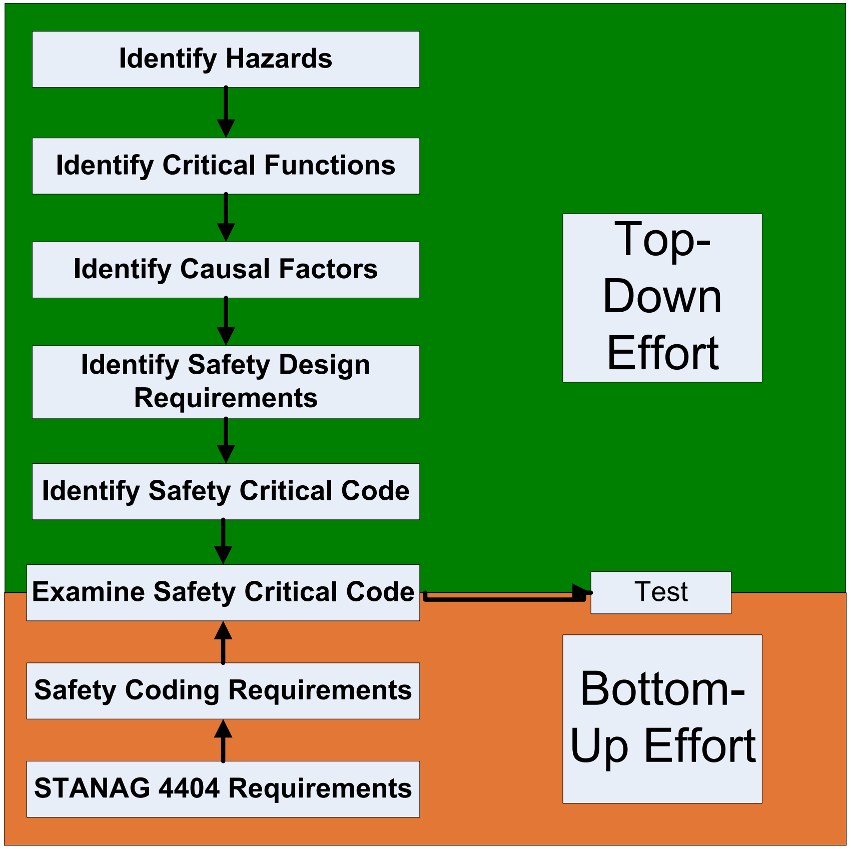
- In software systems stress and strength may be defined in terms of the variate ‘size’. Dimensions of complexity (usually determined in the static domain) can be correlated to size. With stress and strength related, it is possible to describe the reliability in terms of applied stress.

- Safety factors could employed as a design requirement, and as a concession to uncertainties in projecting the ‘strength’ density function
  - Regardless of the execution or stress, the safety factor would ensure a statistically bound likelihood that the overall system would not fail
  - This would satisfy many customer requirements

Backup

Process and Product System Safety

- System analysis uses both "top-down" and "bottom-up" approaches
  - Product: geneally "top-down"
    - Fault tree
    - Hazard Analysis
    - Causal analyses - predecessor causes which directly produce failures
  - Process: generally "bottom-up" compliance & design standards, inspections, process controls
    - Requirements
    - Development standards
    - Code and test reviews
- Guidelines provided in DO-178C, MIL-STD-882 & STANAG 4404 Safety Processes, and other references



Identify Hazards
Identify Critical Functions
Identify Causal Factors
Identify Safety Design Requirements
Identify Safety Critical Code
Examine Safety Critical Code
Test
Safety Coding Requirements
STANAG 4404 Requirements
Top-Down Effort
Bottom-Up Effort

Neither method assesses probabilities of failure under stressing conditions

Deficiencies of Product & Process Analysis

- Systems may have behaviors that are not evident at the component level
  - For example, software can contain a fault(s), that is capable of producing a failure during execution
- Systems may experience events which cause unsafe combinations of external and internal operating conditions
- Product and Process analyses do not provide predictive assessments for customer safety requirements

System Operational Profile

- System operational profile characterizes as a probability function how the software will be used.
- Lists all possible operations the software can realize, and the probability of occurrence of each
- Systems with multiple modes and profiles can be aggregated such that the overall set of modes is expressed as a probability density function