N93-31568

[redacted]

SYSTEM RELIABILITY AND RISK ASSESSMENT TASK GOALS & STATUS

T.A. Cruse and S. Mahadevan
Vanderbilt University
Nashville, Tennessee 37235

The major focus for continued development of the NESSUS codes is in support of system testing and certification of advanced propulsion systems. Current system certification procedures place a major emphasis on design methodology and on system testing. However, as a result of the standard certification effort, no specific levels of system reliability and confidence can be made. Experience in past system development and reliability is used as a guide to determine which tests and how much test time are required for system certification.

Propulsion system testing has evolved over the years from tests designed to show success (benign testing), to tests designed to reveal reliability issues before service use (accelerated testing). Such test conditions as performance envelope corners, high rotor imbalance, power dwells, and overspeed tests are designed to "shake-out" problems that can be associated with low and high cycle fatigue, creep and stress rupture, bearing durability, and the like. Passing these tests by some defined margin of time is intended to indicate a safe operational margin for shorter-term service use of the propulsion system.

Subsystem testing supports system certification by standing as an early evaluation of the same durability and reliability concerns as for the entire system. These tests have to be successful before the full system testing can be initiated. Analysis in support of design is often confirmed in subsystem testing. However, as in system testing for certification, little has been done to quantify just how much reliability has been demonstrated by these standard forms of design analysis, component, and subsystem tests.

The NESSUS software system is being further developed to support the definition of rigorous subsystem and system test definition and reliability certification. The approach taken is a building-block approach, wherein the foundation is constructed before the penthouse - full certification support. The first level of required analysis is that of component reliability (NESSUS 5.0). This analysis has defined the full range of component reliability modeling capabilities, including the consequences of component failure (risk). The NESSUS 5.0 code allows the user great flexibility in choosing critical structural performance and reliability measures, including the impact of reliability of on performance and availability measures.

Current NESSUS 6.0 effort focuses on a variety of issues related to the integration of component reliability information to a system level. In this case, system refers to an assembly of structural components. The current paper outlines the principal technical issues related to system reliability, including key technology issues such as failure mode synergism, sequential failure mechanisms, and fault tree definition. An approach is given to the development of an automatic means for system reliability calculations that includes a definition of the most probable failure [illegible]ences, as well [illegible]ility of system failure. Critically, the proposed method also preserves the sensitivity linkage of each event to all precursor primitive system variables that contribute to system failure. The proposed approach represents a major advance in system reliability, and builds on the available NESSUS analysis strategies.

Quantification of system reliability and sensitivity factors for sequential failures is an essential ingredient in system certification. It is critical to be able to identify failure sequences and to link each with the driving system variables in order to assess critical test conditions and confidence levels for certification. It is also believed that the proposed strategies will provide, for the first time, a basis for a system certification with quantification of reliability measures, as well as a means for defining critical reliability testing requirements. Sensitivity information can be used in a direct manner to define lower confidence intervals on certification testing results.

The paper reports on the proposed solution algorithms which build on previous NESSUS code structures to define the most probable failure sequence(s). Additionally, the paper defines potential approximation schemes for the definition of failure sequences in a cost effect manner. This task is one of the most critical in terms of technology advance for NESSUS 6.0.

SYSTEM RELIABILITY AND RISK ISSUES

1. Component reliability under interaction of all failure modes
2. Conditional dependence between reliabilities of two components
3. Effect of component unreliability on system performance
4. Effect of component unreliability on system availability
5. Effect of component unreliability on life cycle cost
6. System certification requirements

DISCRETE VS. CONTINUUM SYSTEMS RELIABILITY

Present methods → Series/parallel combination of discrete component reliabilities

→ Structural redundancy, correlation of failure modes etc. have been considered

→ No consideration of requential damage

Propulsion systems → Little or no redundancy

→ Sequential damage distributed in the continuum

→ Interaction of failure modes and synergism

→ New strategies required for system reliability computation

SYSTEM RELIABILITY COMPUTATIONS NEEDED FOR CERTIFICATION ANALYSIS

(1) Probability of failure of an individual component due to interacting multiple failure modes (e.g., creep and LCF)

(2) Probability of failure of one component due to failure of another component (e.g., plastic deformation of hot gas seal → causes hot gas leakage → causes reduced thermomechanical fatigue life of another component)

(3) Probability of failure of the system due to failure of multiple components (e.g., fatigue fracture of disk due to combination of cracking in firtrees, rim slots, snap fillets, and bore region)

(4) Probability of failure of multiple components due to a system condition (e.g., temperature, rotor speed)

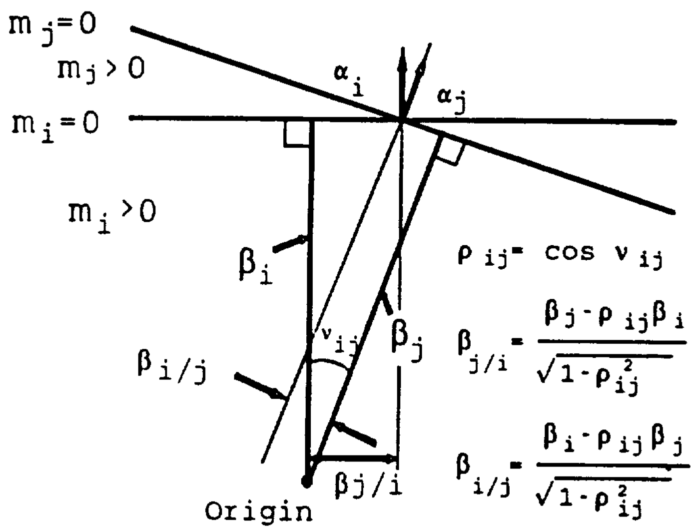
FOUR LEVELS OF COMPUTATIONAL COMPLEXITY ADDRESS SYSTEM RELIABILITY ISSUES

1. Level 0: Independent components/failure modes
2. Level I: Correlations among component failures
   Series/parallel combinations
   Fault tree analysis
3. Level II: Global response surface approach to find joint failure probability
4. Level III: Conditional dependencies between component failures based on sensitivity information and system reanalysis

↓

Alternate System Reliability Method

DITLEVSEN'S APPROXIMATION FOR CONDITIONAL RELIABILITY BASED ON FIRST ORDER SENSITIVITY MODELS



DEFICIENCIES IN DITLEVSEN'S METHOD FOR SYSTEM CERTIFICATION MODELING

1. Applicable to systems with discrete components
2. Does not account for progressive, synergistic damage processes
3. Similar to linear structural analysis
   - → Based on first-order approximation of limit state
   - → Component reliabilities are first found independently and then combined
   - → Does not recognize sequential failure
   - → Does not account for drastic modifications in structural behavior due to failure
4. Possible improvements
   - → Importance Sampling
   - → Formulation of Conditional Limit States
   - → Proposed Alternative Method

PROPOSED ALTERNATE SYSTEM RELIABILITY METHOD ADDRESSES SEQUENTIAL FAILURE MODES

0. Define system and non-system failure modes.

1. ι=0. Determine the reliability of all components.

   –Analyze system model with all random variables.

   –Use perturbation and FPI to find MPP for each failure mode for each component.

2. System failure = Combination of individual system failures
   + Conditional effect of other non-system failures

   Update system reliability result as each system failure mode is encountered.

   Proceed to step 3 with non-system modes.

3. $\iota = \iota + 1$. Impose each non-system failure condition.

   Compute conditional probability of each remaining mode.
   –Perturb the system at the imposed failure condition.
   –Similar to AMV procedure.

PROPOSED ALTERNATE SYSTEM RELIABILITY METHOD ADDRESSES SEQUENTIAL FAILURE MODES (CONTINUED)

4. Repeat steps 2 and 3 until convergence in system reliability result.

5. Define the most probable failure sequence.

6. Define sensitivity of "top-event" to component and system primitive variables (certification issue).

PROPOSED SYSTEM RELIABILITY METHOD PROVIDES UNIQUE TECHNOLOGY ADVANCES

1. Rigorously identifies the most probable failure sequence

   →Construction of fault-tree (bottom-up approach)

2. Also supports top-down approach

   –Sensitivities of various system failure modes to individual component failure modes computed and stored

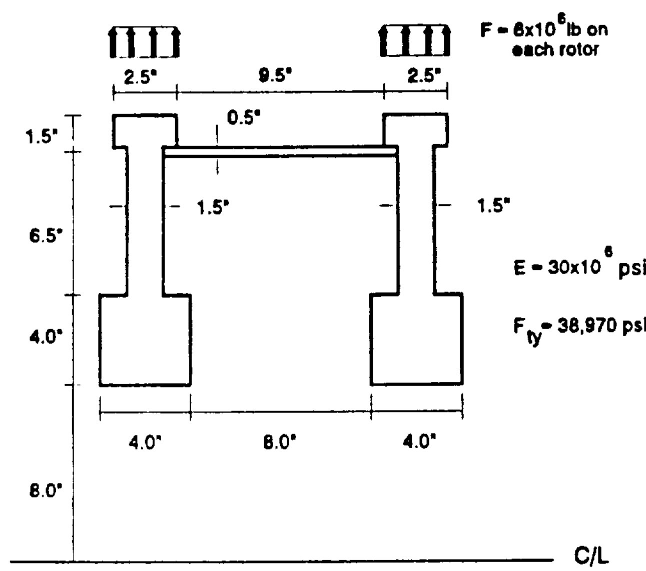
   –Easy identification of the most probable damage, its location and extent that causes system failure

   –Reanalysis after each failure condition ensures that no component failure mode is missed

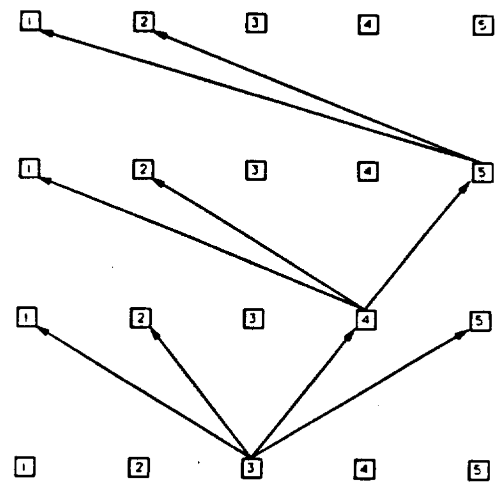
   –Definition to nonlinear structural analysis

   –Modification in structural behavior after each failure is accounted for

EXAMPLE



ONE POSSIBLE SEQUENCE OF REANALYSES



1-- Burst of rotor 1 (System Failure)

2-- Burst of rotor 2 (System Failure)

3-- Yield of rotor 1 (Non-system Failure)

4-- Yield of rotor 2 (Non-system Failure)

5-- Yield of spacer ring (Non-system Failure)

PROPOSED STRATEGIES TO REDUCE COMPUTATIONS

1. Follow the path whose failure modes have highest probability in each step

   →Useful to construct most probable sequence

   →Unsafe for overall system reliability result

2. Use cut-off values for updated failure probabilities

3. Use cut-off values for conditional probabilities

   →PNET Method (Ang)

4. Construct a first-order fault-tree based on sensitivities at $\iota = 0$ (individual component reliability analyses), and pursue significant paths.

STRATEGIES 1 AND 2

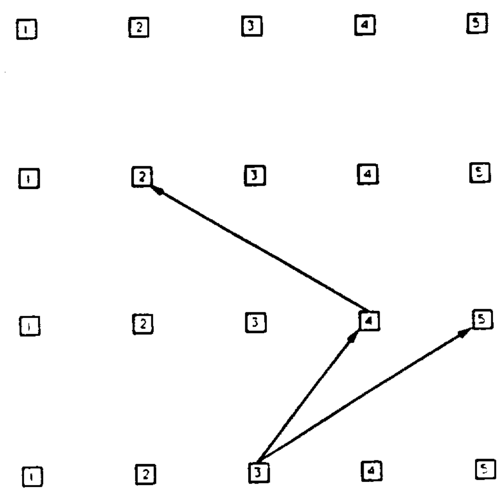
1-- Burst of rotor 1

2-- Burst of rotor 2

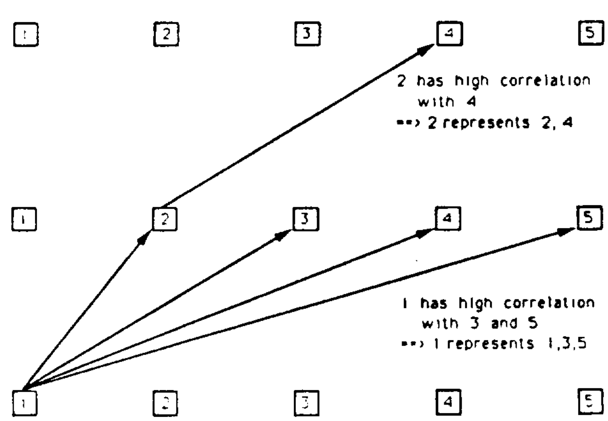
3-- Yield of rotor 1

4-- Yield of rotor 2

5-- Yield of spacer ring



PNET METHOD



P(system failure) = P(1 U 2 U 3 U 4 U 5)

= P(1 U 2)

PROGRAMMING REQUIREMENTS DEFINED

1. User needs to identify all the failure modes
   →system and non-system

2. Code to compute reliabilities for all failure modes at first.

3. Options for most probable failure sequence:
   –Code constructs a first-order fault tree
   –AMV-type reanalysis and refinement for dominant paths
   –User is allowed to eplore a chosen sequence

4. Store and receive
   –MPP for each failure mode
   –Sensitivities of each failure mode to random variables
   –Conditional probability of each failure mode to previous modes in a sequence

5. Output
   –System reliability update at each step
   –Subsystem conditional failure probabilities at each step
   –Most probable failure sequence

APPLICATION TO PROPULSION SYSTEM CERTIFICATION

1. Compute reliability effects on system perfomance, life cycle cost, and availability

2. Link system reliability analysis with CLS (Composite Load Spectrum)
   –Sensitivity information regarding loads and performance
   –e.g., hot gas seal leakage

3. System reliability analyses include failed conditions
   –Need to recompute sensitivity information

4. Definition of system certification testing requirements
   –Sensitivity information needed to determine
      (i) confidence bounds
      (ii) accelerated testing parameters

5. System reliability analysis can account for "unknown-unknowns"
   –design and assembly errors
   –sequential failure nodes
   –functional failures