602401

Summary of Research on Reliability Criteria-Based Flight System Control

N. Eva Wu

Department of Electrical Engineering

Binghamton University

Binghamton, NY 13902-6000

607-777-4375, evawu@binghamton.edu

Cooperative Agreement: NCC-1-336.

Tech POC: Dr. Christine Belcastro, NASA Langley.

Support period: February 1, 1999-January 31, 2002.

Outline

- Overview of project focuses
- Reliability analysis
  - Role of reliability analysis in AvSP
  - Contributions
  - Some remarks
  - Challenges
- Design for reliability
  - Design issues
  - Contributions
  - Cost constrained reliability allocation(recent work)
  - Some thoughts on future research

Overview of Project Focuses

- Develop methods and select tools for reliability assessment of adaptive flight control systems
- Develop methods for modeling the controlled flight system recovery process and evaluating the likelihood of success
- Develop integrated adaptive control synthesis methods based on reliability criteria

Reliability Analysis

- Role of reliability analysis in AvSP
  - Identify and quantify the needs for aviation safety enhancement
  - Specify the safety goals and measures
  - Set an all encompassing criterion and guidelines for integrated system designs
  - Provide tools for validation and verification of modified and new designs aimed at reliability enhancement
  - Bottom line
    - Establish measures through scientific means that are convincing to ourselves and others on what needs to be and has been accomplished

Reliability Analysis

- **Contributions**
  - **Surveyed reliability assessment tools and selected candidate tools to be used for AvSP**
    - ➢ Software tools: http://www.enre.umd.edu/tool.htm
    - ➢ Rationale for the selection of SURE & ASSIST (summer'99 report)
      - ◆ Handle complex reconfiguration strategies with simple reliability models (no reason for complex models due to lack of data)
      - ◆ Provide accuracy for disparate failure and recovery rates
      - ◆ Have flexibility to allow incorporation of decision risk factors
      - ◆ Require a thorough understanding of failure and recovery processes
    - ➢ Possible improvement: more user friendly interface
      - ◆ Suggest that AvSP support such an endeavor if Ricky is willing (SURE is of very high quality and unique work)

Reliability Analysis

- **Contributions (cont'd)**
  - ➢ Systems to which SURE & ASSIST are applied
    - ◆ A flight control system (to apepar ACC'02)
      - » Sensitivity analysis w.r.t. hazard rate, redundancy level, coverage, removal rate using SURE
    - ◆ An industrial process
  - ➢ Lessons learnt
    - ◆ Functional redundancy can greatly enhance system reliability
    - ◆ But the benefit can be severely compromised by inadequate coverage
    - ◆ Adequate coverage: 1-coverage hazard rate
  - ➢ Some recommendations
    - ◆ Some hardware redundancy can be reduced
    - ◆ A focused effort to enhance coverage is needed

Reliability Analysis

- **Contributions (cont'd)**
  - **Incorporated decision risk factors brought in by added safety enhancement features through the notion of coverage**
    - ➢ **Characteristics of coverage**
      - ◆ **Often dominating the overall system reliability**
      - ◆ **Difficult to model**
      - ◆ **Highly scenario dependent**
      - ◆ **Highly time dependent**
    - ➢ **An example of coverage estimate: acc'00 paper**
    - ➢ **Propose similar criteria set for all new designs and new systems aimed at safety enhancement**

Reliability Analysis

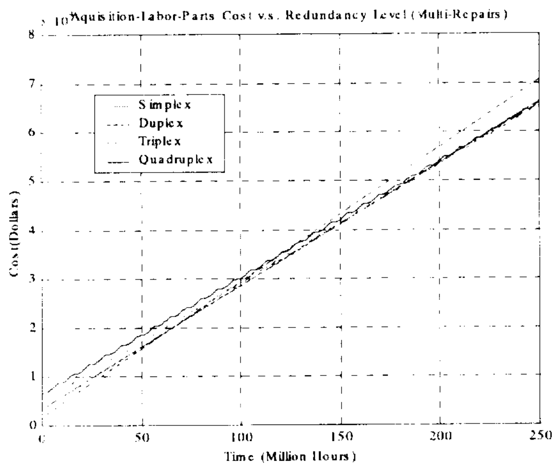
- **Contributions (cont'd)**
  - **Exploited conditions peculiar to AvSP applications and derived a number of bounding relations that provide insight and simplifications to reliability analysis**
  - **Examples of results**
    - ◆ **: hazard rate of a subsystem (10^{-6}~10^{-4} $hour^{-1}$)**
    - ◆ **: maximum MTTR of a faulty subsystem (10^{-4}~10^{-3} hour)**
    - ◆**T: mission time (10^{0}~10^{1} hour)**
    - ◆**k-out-of-n: k operational out of n parallel configuration**
    - ◆**c_0: coverage of the first failure (0.9~0.999999)**
  - ➢ **P n T(1-c_0) if n T<<1, and**

$$1 \quad c_0 \qquad \frac{(n \quad 1) \quad [(1 \quad T)^n \quad 1] \quad [(1 \quad T)^n \quad (1 \quad nT)]}{n \; T(1 \quad n \; T \,/\, 2)}$$

  - ➢ **MTTR can be ignored if (1-c_0)>> n**

Reliability Analysis

- **Contributions (cont'd)**
  - **A preliminary study on economic considerations**
    - ➢ **Suggest that AvSP support the development and test of the study**
    - ➢ **Propose to develop cost analysis for need-based maintenance**

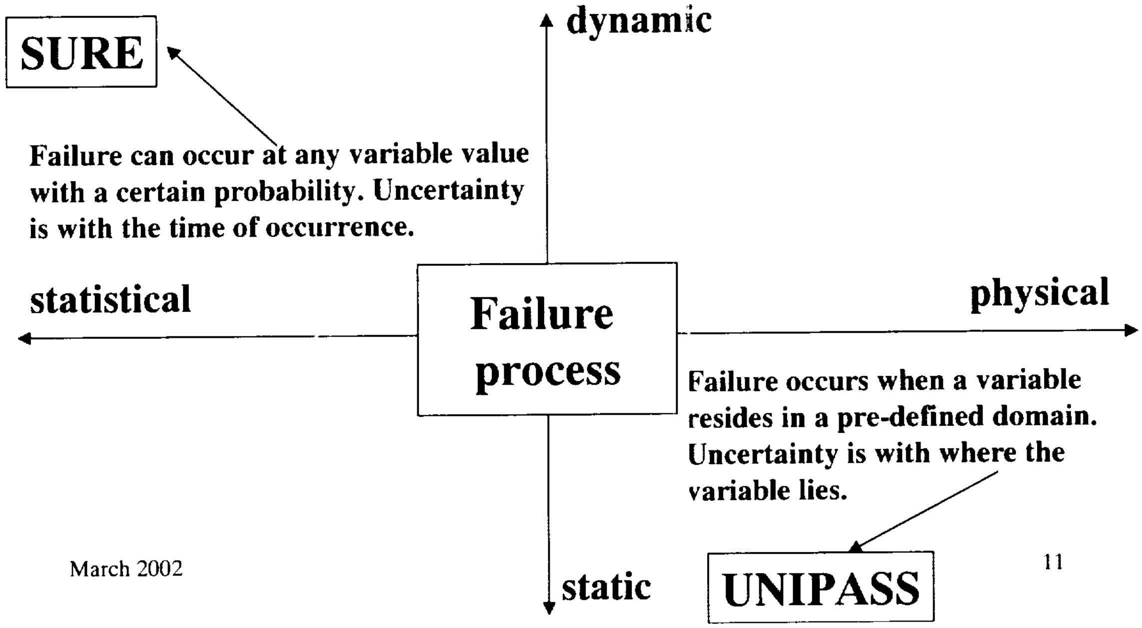


Reliability Analysis

- **Contributions (cont'd)**
  - **Investigated applicability of UNIPASS in AvSP (summer'01 report)**
    - ➢ **Failure probability analysis for components** **(known LSF & JPDF)**
      - ◆**Good prediction when component LSFs have small uncertainties**
      - ◆**Help dynamic reliability modeling through covariate methods**
      - ◆**Provide useful information for feedback control (Sean Kenny)**
    - ➢ **Identify needs and the potential for component reliability enhancement**
      - ◆**Sensitivity analysis**
    - ➢ **Difficulties**
      - ◆**Joint probability distribution model for components**
      - ◆**Randomized limit state treatment**

Reliability Analysis

- Contributions (cont'd)
  - UNIPASS v.s. SURE



Reliability Analysis

- Challenges
  - *Test* data crucial to reliability study but sensitive from market-competition & liability viewpoints are difficult to obtain, while *accident* data alone are not sufficient (propose to partially mitigate data deficiency through control)
  - New reliability measure/assessment tools that can provide more accurate information under less stringent data requirements are yet to be defined/developed (propose to use imprecise probabilities)
  - Lack of existing tools for fault coverage modeling and decision risk assessment for aviation safety (a solution obtained, but not yet tested on a real system)

Design for Reliability

- **Design issues**
  - **Make use of existing redundancy**
    - ➢ Secondary functions
    - ➢ Projections
    - ➢ Virtual variables
  - **Ongoing effort**
    - ➢ Diagnosis and monitoring
    - ➢ Fault tolerant control
  - **Recent effort**
    - ➢ Reliability allocation

Design for Reliability

- **Contributions**
  - **System monitoring and diagnosis**
    - ➢ Developed an adaptive parameter estimation algorithm that has been tested on a nonlinear vehicle model for identification of additive, multiplicative, and incipient faults (IJACSP, 2000)
    - ➢ Proposed a pulse compression method for system monitoring (ACC, 2001)
    - ➢ Introduced diagnostic resolution as a measure for the performance of diagnostic systems, through which a functional relation to system reliability is established (IJSS, 2000)
    - ➢ Defined a redundancy measure that quantifies the extent the redundancy can be utilized for failure recovery through feedback control (Automatica, 2000)

Design for Reliability

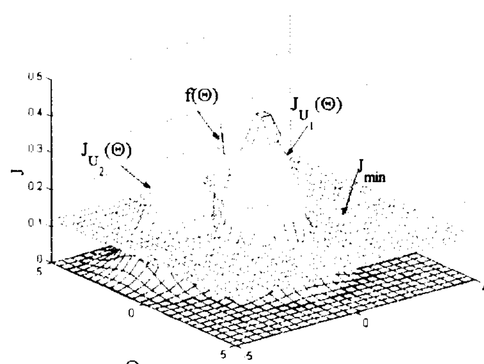
- **Contributions (cont'd)**
  - **Fault tolerant control**
    - ➢ **A proof of concept fault-tolerant control was performed using a linear parameter varying model scheduled with respect to fault effects and a polytopic control method (DASC, 2000)**
    - ➢ **A multiple channel configuration using a decentralized adaptive control approach to fault tolerance was proposed and an initial design was attempted on the 6 DOF nonlinear aircraft model (SafeProcess, 2000)**
    - ➢ **A quantitative relation was established between the control performance and the overall system reliability through fault coverage (IJSS, 2000)**
    - ➢ **Concepts of dynamic coverage, crucial for on-line decision making, and static coverage, crucial for reliability assessment and for specifying subsystem performance, were introduced (CDC, 2001)**

Design for Reliability

- **Contributions**
  - **Definition of coverage**

$$C_{U_i} \quad \underset{i}{\quad} f(\ )d\ , \quad i \quad |J_{U_i}(\ )\ \ J_{min}$$

  - **Some recent results (CDC, 2001)**
    - ➢ **A more robust control law results in a higher coverage**
    - ➢ **A higher resolution diagnostic scheme results in a higher coverage**
    - ➢ **A less stringent control performance requirement results in a higher coverage**
  - **A proof of concept design for HIMAT under the max coverage criterion**
    - ➢ **Propose to perform an evaluation for the NASA B757**



Design for Reliability

- **Reliability allocation**
  - **Problem formulation**

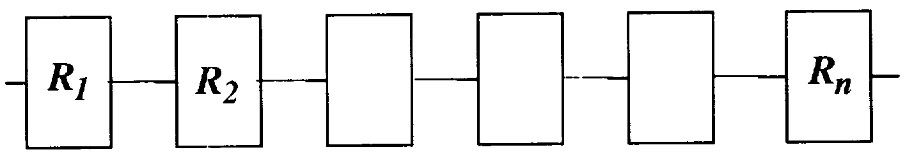
$max\, R_{\text{system}}^{\text{new}} \quad f^{\text{new}}(R_1 \quad R_1, R_2 \quad R_2, \cdots, R_n \quad R_n) \quad R_{\text{required}}$

$f^{\text{old}}(R_1, R_2, \cdots, R_n) \quad R_{\text{system}}^{\text{old}}$ where $0 \quad R_i \quad R_i \quad 1, \; i \quad 1,2,\cdots,n$

subject to

$C_1(\quad R_1) \quad C_2(\quad R_2) \quad \cdots \quad C_n(\quad R_n) \quad C_{max}$

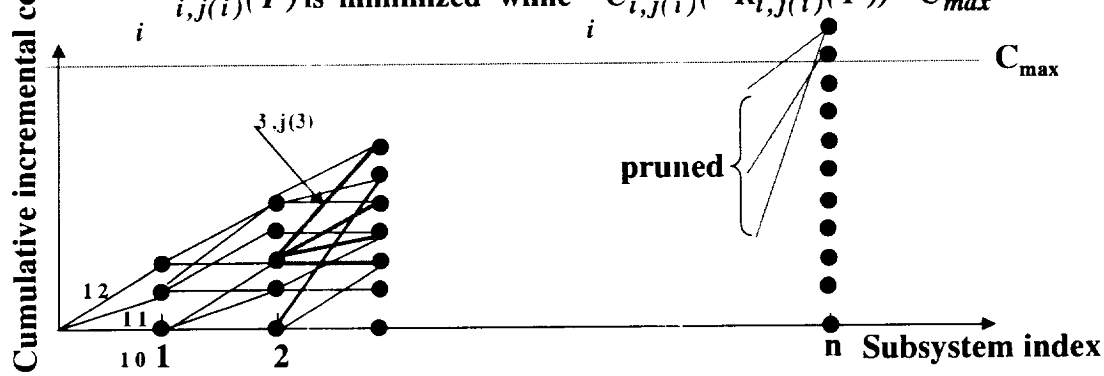
Flight critical processors | I/O control modules | Pilot command sensors | Aircraft state sensors | Lateral directional effectors | Longitudinal effectors



Design for Reliability

- **Solution to reliability allocation via constrained optimization**
  - ➢ n subsystems
  - ➢ m_i configurations for subsystem i
  - ➢ $R_{i,j}(T)$: reliability of the j^{th} configuration of the i^{th} subsystem at T
  - ➢ $_{i\,j}(T)$: T-equivalent hazard rate of the j^{th} configuration of the i^{th} subsystem $\quad _{ij}(T) \quad \ln R_{ij}(T) \quad R_{ij}(T)\; T^{\;1}$

$\underset{i}{} \; _{i,j(i)}(T)$ is minimized while $\underset{i}{} \; C_{i,j(i)}(\quad R_{i,j(i)}(T)) \quad C_{max}$



- ➢ propose to perform an RR study for the NASA B757

Design for Reliability

- **Some thoughts on future research (cont'd)**
  - **All reported results should be tested on a realistic test-bed or a realistic set of aircraft data selected for AvSP for verification and demonstration of methods**
  - **Reliability analysis based on imprecise probability**
    - ➢ **Needs**
      - ◆ **lack of sufficient statistics**
      - ◆ **lack of precision and consistency in expert opinion**
      - ◆ **large uncertainty in pilots' decisions**
    - ➢ **Issues**
      - ◆ **uncertainty description, arithmetic, measure, and principles**
      - ◆ **rule of combination**
      - ◆ **robustness**

Design for Reliability

- **Some thoughts on future research (cont'd)**
  - **Global control reconfigurability for non-analytic models**
    - ➢ **Control reconfigurability?**
      - ◆ **Ability of vehicle to allow restoration of stability through feedback control**
    - ➢ **Needs**
      - ◆ **Reveal potentiality and limitation of feedback control, system condition criticality, subsystem dependency, ... , so that vehicle recoverability can be fully exploited and loss of vehicle control can be prevented**
    - ➢ **Feasibility**
      - ◆ **Low fidelity and incomplete data can allow assessment of reconfigurability**
    - ➢ **Issues**
      - ◆ **Locality (domain expansion)**
      - ◆ **Singularity (gap-metric based approximation)**
      - ◆ **Directionality (mode specific reconfigurability)**
      - ◆ **Computability (convex optimization)**
  - **New adaptive control strategies**

    (initial work submitted to GNC'02 in collaboration with Shin and Belcastro)