RELIABILITY ASSESSMENT OF RECONFIGURABLE FLIGHT CONTROL SYSTEMS USING SURE AND ASSIST

N. EVA WU

DEPARTMENT OF ELECTRICAL ENGINEERING
BINGHAMTON UNIVERSITY
BINGHAMTON, NEW YORK 13902-6000, USA
TEL: (607) 777-4375
FAX: (607) 777-4464
EMAIL: EVAWU@BINGHAMTON.EDU; N.E.WU@LARC.NASA.GOV

OBJECTIVES

- DEVELOP RELIABILITY ASSESSMENT TOOLS
  - SOPHISTICATED SYSTEM CONFIGURATION
  - MULTIPLE SOURCES OF UNCERTAINTY

- SURE: SEMI-MARKOV UNRELIABILITY RANGE EVALUATOR
  — APPLICABLE TO A LARGE CLASS OF SEMI-MARKOV MODELS
  — EFFICIENT AND ACCURATE
  — AVAILABLE FOR VMS/UNIX/MS-WINDOWS OS

- ASSIST: ABSTRACT SEMI-MARKOV SPECIFICATION INTERFACE TO THE SURE TOOL
  — MODEL GENERATION TOOL FOR DIRECT INTERFACE WITH SURE
  — POWERFUL AID TO MODELING COMPLEX SEMI-MARKOV PROCESSES
  — AVAILABLE FOR VMS/UNIX/MS-DOS OS

JUSTIFICATION FOR FURTHER COMPUTATION SIMPLIFICATIONS

ON-LINE DECISIONS

UTILITY
• SOME BACKGROUND

○ MARKOV PROCESS\[7\]:
\[
\{X(t) \mid t \in (0, \infty)\} \text{ IS A MARKOV PROCESS IF } \forall t_0 < t_1 < \cdots < t_n < t, \text{ THE CONDITIONAL DISTRIBUTION OF } X(t) \text{ FOR GIVEN VALUES OF } X(t_0), \cdots, X(t_n) \text{ DEPENDS ONLY ON } X(t_n)
\]
\[
P(X(t) \leq x \mid X(t_n) = x_n, \cdots, X(t_0) = x_0) = P(X(t) \leq x \mid X(t_n) = x_n)
\]

* HOMOGENEOUS MARKOV PROCESS:
\[
P(X(t) \leq x \mid X(t_n) = x_n) = P(X(t - t_n) \leq x \mid X(0) = x_n)
\]

—WHITE’S INTERPRETATION:
CONSTANT RATE
INDEPENDENT COMPETING EVENTS
INDEPENDENT SEQUENTIAL EVENTS
⇒
\[
F(t) \text{ (TIME A PROCESS SPENDS IN A STATE) IS EXPONENTIAL}
\]
\[
P(T \leq t) = F(t) = 1 - e^{-\lambda t}
\]

* SEMI-MARKOV PROCESS: A MARKOV PROCESS WHOSE DISTRIBUTION IS NOT EXPONENTIAL.

○ EXAMPLE: AFTI/F-16 FAULT TOLERANT FCS[10]

![Diagram of Functional dependency of subsystems in the FTFCS]

- A PARALLEL-TO-SERIES INTERCONNECTION OF 5 BLOCKS
- FLIGHT CRITICAL PROCESSES
- POWER SUPPLIES, DIGITAL PROCESSORS
- I/O CONTROL MODULE
- PILOT COMMAND SENSOR
- AIRCRAFT STATE SENSOR
- EFFECTOR
- ACTUATORS, SURFACES, INTERFACE UNITS
• SOME PROPERTIES OF THE RELIABILITY MODEL
  ◦ BUILDING BLOCKS: SUBSYSTEMS (NO SPARES, NO REPAIRS)
  ◦ REDUNDANCY TYPE: HARDWARE AND FUNCTIONAL
  ◦ FAILURE: CONTROL PERFORMANCE DEPENDENT
    - SUBSYSTEM FAILURE
      LACK OF REDUNDANT CONTROL AUTHORITY
  ◦ FAILURE DETECTION: RESIDUE BASED
    - RESIDUALS ARE NOISY
    - RECONFIGURATION DECISIONS INVOLVE RISKS
  ◦ MISSION TIME $t_m$: SHORT
  ◦ HOLDING TIME DISTRIBUTION $F(t)$: DIFFICULT TO DETERMINE
    - NO BASIS FOR ASSUMING EXPONENTIAL
    - POSSIBLE TO BOUND BY EXPONENTIAL DISTRIBUTIONS
      \[ 1 - e^{-\lambda_1 t} \leq F(t) \leq 1 - e^{-\lambda_2 t}, \quad t \leq t_m \]
  ◦ WHAT TO EXPECT?
    - RIGHT ORDERS OF MAGNITUDE
  ◦ PROPERTIES (CONT'D) PECULIAR TO FUNCTIONAL REDUNDANCY
  ◦ SYSTEM ARCHITECTURE: MORE COMPLEX IN GENERAL
  ◦ LESS SYMMETRY ⇒ HARDER TO OBTAIN A RELIABILITY MODEL
  ◦ DEATH STATE: DICTATED BY RELIABILITY REQUIREMENTS
  ◦ INOPERATIVE WITH MAJORITY
  ◦ OPERATIVE WITHOUT MAJORITY
  ◦ NO.1 CAUSE OF DEATH ⇒ UNSUCCESSFUL RECONFIGURATION
    - FALSE ALARM
    - MISS DETECTION
    - FALSE IDENTIFICATION
    - FALSE RECONFIGURATION
  ◦ EXHAUSTION OF FUNCTIONAL REDUNDANCY
  ◦ COVERAGE $C(t)$: NECESSARY
    - HIGHLY SCENARIO DEPENDENT;
    - VERY DIFFICULT TO ESTIMATE;
    - HIGHLY TIME DEPENDENT;
    - HARD TIME LIMIT ($t_{max}$ < DEPARTURE TIME)
      \[ C(t) \approx C(t_{max}) \]
• AN EXAMPLE OF CALCULATED COVERAGE
  ○ SCENARIO — 75% LOSS OF CANARD EFFECTIVENESS
  ○ DATA
    — MODEL OF THE AIRCRAFT
      MEASURED ANGLE OF ATTACK AND PITCH ANGLE
    ○ FACTORS AFFECTING THE VALUE OF COVERAGE
      — PERFORMANCE OF CONTROL, DIAGNOSTIC, DECISION MODULES
  ○ RESULTS
    — A LUCKY SITUATION OF ACHIEVING 0.9999 AFTER 4.2 SECONDS
      — AT T=0.5S, LOWER BOUND OF COVERAGE IS ONLY 0.75

• RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK
  Semi-Markov process:
  Degradable 4-plex with full reconfiguration

• BLOCK FAILURE PROBABILITY BOUNDS

\[
\lambda = 10^{-5} \\
\mu \in [10^{-4}, 10^{0}] \\
\sigma = 10^{-2} \\
C_{01} = C_{12} = C_{23} = 1 \\
l_m = 1
\]
RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK
RECONFIGURATION IS NOT COMPLETE

Semi-Markov process:
Degradable 4-plex with incomplete reconfiguration

BLOCK FAILURE PROBABILITY BOUNDS

SURE RELIABILITY ANALYSIS OF THE PROCESSOR BLOCK
INSTANTANEOUS REMOVAL OF A FAULTY SUBSYSTEM

Markov process:
Degradable 4-plex with incomplete reconfiguration

BLOCK FAILURE PROBABILITY BOUNDS

\[ \lambda = 10^{-5} \]
\[ \mu = 10^{-1} \]
\[ \sigma = 10^{-2} \]
\[ C_{01} \in [0.99, 1.0] \]
\[ C_{12} \in [0.95, 1.0] \]
\[ C_{23} \in [0.90, 1.0] \]
\[ t_m = 1 \]
- **EFFECTS OF NEGLECTING REMOVAL TIMES**

  - **BLOCK FAILURE PROBABILITY BOUNDS**

  

  \[ \lambda = 10^{-5} \]
  \[ \mu = 10^{-1} \]
  \[ C_{01} \in [0.99, 1.0] \]
  \[ C_{12} \in [0.95, 1.0] \]
  \[ C_{23} \in [0.90, 1.0] \]
  \[ t_m = 1 \]

- **FURTHER SIMPLIFICATION OF THE PROCESSOR MODEL**

  \[ p_f \approx (1 - C_{01})4\lambda t_m \]

  - **A SYSTEM WITH AN EQUIVALENT FIRST ORDER EFFECT**

  - **BLOCK FAILURE PROBABILITY**

  

  \[ \lambda = 10^{-5} \]
  \[ \mu = 10^{-1} \]
  \[ C_{01} \in [0.99, 1.0] \]
  \[ C_{12} \in [0.95, 1.0] \]
  \[ C_{23} \in [0.90, 1.0] \]
  \[ t_m = 1 \]

- **VALID IF RELATIVE TO THE FAILURE PROCESS**

  - REMOVAL OF FAULTY SUBSYSTEMS IS FAST
  - MISSION TIME IS SHORT
JUSTIFICATION OF 2ND APPROXIMATION

AN $r+1$ STATE MARKOV PROCESS

- $r$ OR MORE FAILED SUBSYSTEMS, OR
- INCORRECT RECONFIGURATION DECISION

SOME NOTATIONS
- $\lambda$: FAILURE RATE OF A SUBSYSTEM
- $t_m$: MISSION TIME
- $p_{ij}(t)$: TRANSITION PROBABILITY
- $C_{ij}$: COVERAGE OF A TRANSITION

FAILURE OF AN $n$-SUBSYSTEM BLOCK

COMBINATORY APPROACH

$P(t) = \begin{pmatrix}
    p_{00}(t) & p_{01}(t) & p_{02}(t) & \cdots & p_{0r}(t) \\
    0 & p_{11}(t) & p_{12}(t) & \cdots & p_{1r}(t) \\
    0 & 0 & p_{22}(t) & \cdots & p_{2r}(t) \\
    \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & \cdots & 0 & \cdots & p_{rr}(t)
\end{pmatrix}$

$p_{ij}(t) = \binom{n-i}{j-i} q^{i-j}(1-q(t))^{n-i} C_{ij}, \quad i \leq j < r$

$p_{ij}(t) = 0, \quad i > j$

$p_{ir}(t) = 1 - \sum_{j=i}^{r-1} p_{ij}(t), \quad 0 \leq i \leq r - 1$

$p_{rr}(t) = 1$

$q(t) = (1 - e^{-\lambda t})$

IS THE SUBSYSTEM FAILURE PROBABILITY

TRANSITION RATE MATRIX $Q = \dot{P}(t)$
AN ALTERNATIVE WHEN \( Q \) IS KNOWN

\[
\dot{P}(t) = P(t)Q(t)
\]

WHERE

\( P_{(r+1)\times(r+1)} \) IS THE P.T.M.
\( Q_{(r+1)\times(r+1)} \) IS THE T.R.M.

\[
P_f = [P(t)]_{(1,r+1)}, \quad t \leq t_m
\]

COMPOSITE FAILURE PROBABILITY

OF \( m \) CASCADED BLOCKS

\[
1 - \prod_{i=1}^{m} \{ 1 - [P_i(t)]_{(1,r+1)} \}
\]

\[
\begin{pmatrix}
-n\lambda & C_0 n\lambda & 0 & \cdots & 0 \\
0 & -(n-1)\lambda & C_1 (n-1)\lambda & 0 & \cdots \\
0 & 0 & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & -(n-r)\lambda & (n-r+1)\lambda \\
0 & \cdots & 0 & 0 & 0
\end{pmatrix}
\]

\( Q \) INDEPENDENT OF \( t \)

\( \Rightarrow \) HOMOGENEOUS MARKOV PROCESS

\[
P(t) = e^{Q} = e^{P^N(t/N)}
\]

\[
\approx (1 + Q_N t)^N, \quad \text{EULER APPROXIMATION}
\]

\[
\approx (1 + Qt), \quad \text{TAYLOR EXPANSION}
\]

\[
P_f = [P(t_m)]_{(1,r+1)}
\]

\[
\approx [Q]_{(1,r+1)} t_m
\]

\[
= [1 - C_{01}] n\lambda t_m
\]
**APPROXIMATION ERROR**

\[ P_f(t) = |P(t)|_{1,r+1} \]
\[ = [e^{Qt}]_{1,r+1} \]
\[ = \left| \lim_{N \to \infty} \sum_{i=0}^{N} \frac{1}{i!} [(Qt)^i]_{1,r+1} \right| \]

**DEFINE THE APPROXIMATION ERROR**

\[ e = P_f(t) - P_f^{approx}(t) \]

**THEN**

\[ e(t) = \left| \lim_{N \to \infty} \sum_{i=2}^{N} \frac{1}{i!} [(Qt)^i]_{1,r+1} \right| \]

**NOTE THAT**

\[ \left| [(Qt)^i]_{1,r+1} \right| \leq (r + 1)(n\lambda t)^i \]

**THEREFORE**

\[ |e| \leq \left| \lim_{N \to \infty} \sum_{i=2}^{N} \frac{1}{i!} (r + 1)(n\lambda t)^i \right| \]
\[ \leq \frac{(r + 1)(n\lambda t)^2}{2} \left| \lim_{N \to \infty} \sum_{i=0}^{N-2} \frac{n\lambda t}{2} \right| \]
\[ = \frac{(r + 1)(n\lambda t)^2}{2 - n\lambda t}, \quad n\lambda t < 2 \]
\[ < (r + 1)(n\lambda t)^2, \quad n\lambda t < 1 \]

**SOME REMARKS**

- **GOOD APPROXIMATION**

\[ (r + 1)(n\lambda t)^2 < < (1 - C_{01})n\lambda t \]

**OR**

\[ C_{01} < 1 - n^2\lambda t \]

- **REdundant system versus simple system**

\[ |1 - C_{01}| n\lambda t_m < \lambda t_m \]

**OR**

\[ C_{01} > 1 - \frac{1}{n} \]

- **In general,** \( 1 - C_{01} \) decreases as \( n \) increases

\[ \Rightarrow \text{there is an } n \text{ at which} \]

\[ \min_n (1 - C_{01}) n\lambda t_m \]

**IS ACHIEVED**

- **EXAMPLE**

**REDUNDANCY MANAGEMENT**

<table>
<thead>
<tr>
<th>( n )</th>
<th>( C_{01} )</th>
<th>( (1 - C_{01})n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0.992</td>
<td>0.032</td>
</tr>
<tr>
<td>3</td>
<td>0.99</td>
<td>0.03</td>
</tr>
<tr>
<td>2</td>
<td>0.89</td>
<td>0.22</td>
</tr>
</tbody>
</table>
ERROR DUE TO NEGLECTING REMOVAL TIMES

Omitted paths to death states

\[ \sum_{i=0}^{n} \frac{n!}{(n-i)!} (1 - e^{-\lambda t})^i e^{-\lambda t} \]

Higher rates to death states

\[ C_{t+1} \rightarrow 1, F_i(t) \rightarrow 1 \]

Approximation error bound

\[ e = p_f - p_{f}^{\text{approx}} < \sum_{i=1}^{\frac{n-1}{2}} \prod_{j=1}^{n-i} (1 - e^{-\lambda t}) e^{-\lambda t} \]

\[ \leq \sum_{i=1}^{\frac{n-1}{2}} \prod_{j=1}^{n-i} (1 - e^{-\lambda t}) = 4 \cdot 3 \lambda^2 t (2 \cdot \lambda t^2 + 2 \cdot \lambda t + 1) \]

\[ < (4\lambda t)^2, \quad (\lambda t) < \frac{1}{8} \]

Good approximation

\[ (1 - C_{01})4\lambda t \gg (4\lambda t)^2 \iff C_{01} \ll 1 - 4\lambda t \]

General error bound for neglecting removal times

\[ e = p_f - p_{f}^{\text{approx}} < \sum_{i=2}^{\frac{n-1}{2}} \frac{n!}{(n-i)!} (1 - e^{-\lambda t})^i e^{-\lambda t} \]

\[ < \sum_{i=2}^{\frac{n-1}{2}} \frac{n!}{(n-i)!} (\lambda t)^i - n(n-1)(\lambda t)^i \sum_{i=0}^{\frac{n-2}{2}} (n-2)(\lambda t)^i \]

\[ = n(n-1)(\lambda t)^2 \left( 1 - \frac{1}{1 - (n-2)(\lambda t)^2} \right) \]

\[ < (n\lambda t)^2, \quad n\lambda t < \frac{1}{n-2} \]

Good approximation

\[ (1 - C_{01})n\lambda t \gg (n\lambda t)^2 \]

OR

\[ C_{01} \ll 1 - n\lambda t \]
● ANALYSIS OF THE EFFECTOR BLOCK

1. C/E means computer/effector interface in triplex/quadruplex configuration
2. 3 out of 4 #1/#2 effectors required
3. Either #3 or both #4 effectors required

● SURE AND ASSIST ARE NEEDED IN HIGH COVERAGE MODELS

● EXAMPLE: DEGRADABLE 2-PLEX CONTAINING 3-PLEX–1-PLEX'S

\[ \lambda_1 = 10^{-5}, \lambda_2 = 5.0 \times 10^{-6}, t_m = 1.0 \]

\[ C_{01}^1 \in [0.99, 1.0] \]
\[ C_{12}^1 \in [0.95, 1.0] \]
\[ C_{23}^1 \in [0.96, 1.0] \]
\[ C_{01}^2 \in [0.99, 1.0] \]

○ A SIMPLIFICATION WITH AN EQUIVALENT FIRST ORDER EFFECT
- \(3\lambda_1\) AND \(\lambda_2\) ARE OF THE SAME ORDERS OF MAGNITUDE
- \(C_{01}^1\) AND \(C_{01}^2\) ARE OF THE SAME ORDERS OF MAGNITUDE

○ SIMPLE FORMULA

\[ P_f = 6\lambda_1|1 - C_{01}^1|t + 2\lambda_2|1 - C_{01}^2|t, \ t \leq t_m \]
**Using Assist and Sure**

("Markov model generation for a 2-channel 1-plex -> 1-plex degradable configuration")

("Failure rates and coverage")

LA = 0.5; "Subsystem failure rate for block A (1-plex block)")

LB = 0.6; "Subsystem failure rate for block B (1-plex block)")

CA1 = 0.9; "Coverage for the 1st failure in block A")

CA2 = 0.9; "Coverage for the 2nd failure in block A")

CA3 = 0.9; "Coverage for the 3rd failure in block A")

CB1 = 0.9; "Coverage for the failure in block B")

(* Input to SURE for coverage variation *)

DELTA = 0.0 TO + 1.0;

(* Delta t is the coverage range = step size *)

CA1 = 0.95 * DELTA + 0.05;

(* CA1 ranges from 0.95 to 1.0 *)

CA2 = 0.95 * DELTA + 0.05;

(* CA2 ranges from 0.95 to 1.0 *)

CB1 = 0.95 * DELTA + 0.05;

(* CB1 ranges from 0.95 to 1.0 *)

State space definition (Array of two identical channels)

SPACE = (NCA, ARF_A[I..2] OF 0..3, NFA, A_RAY[I..2] OF 0..3, NUA, A_RAY[I..2] OF 0..1, NCB, A_RAY[I..2] OF 0..1, NFB, A_RAY[I..2] OF 0..1)

"NCA = Number of operational subsystems in block A")

"NFA = Number of inoperative subsystems in block A")

"NUA = Flag uncovered failures in block A when NUA=1")

"NCB = Number of operational subsystems in block B")

"NFB = Number of inoperative subsystems in block B")

(* Initial state definition *)

START = (2 OF 3, Z OF 0, 2 OF 0, 2 OF 0, 20 OF 0);

(* Failure state definition *)


(* State transitions in channel I, I=1,2 *)

IF (NUA[I] = 0 AND NFA[I] = 0) THEN (* No failures in block A *)

TRANS (NCA[I]=NCA[I]-1, NFA[I]=NFA[I]-1) BY NCA[I]*LA[I]*CA[I]; (* covered *)

ENDIF

IF (NUA[I] > 0 AND NFA[I] = 0) THEN (* 1st failure in block A *)

TRANS (NCA[I]=NCA[I]-1, NFA[I]=NFA[I]-1) BY NCA[I]*CA[I]*CA[I]; (* covered *)

ENDIF

IF (NUA[I] = 0 AND NFB[I] = 0) THEN (* Failure in block B *)

TRANS (NCA[I]=NCA[I]-1, NFA[I]=NFA[I]-1) BY NCA[I]*CA[I]*CA[I]; (* covered *)

TRANS (NCA[I]=NCA[I]-1, NFB[I]=NFB[I]-1) BY NFB[I]*CA[I]*CA[I]; (* covered *)

ENDIF

IF (NUA[I] > 0 AND NFB[I] = 0) THEN (* 1st failure in block B *)

TRANS (NCA[I]=NCA[I]-1, NFA[I]=NFA[I]-1) BY NCA[I]*CA[I]*CA[I]; (* covered *)

TRANS (NCA[I]=NCA[I]-1, NFB[I]=NFB[I]-1) BY NFB[I]*CA[I]*CA[I]; (* covered *)

ENDIF

FINITE REMOVAL TIMES CAN BE EASILY INCORPORATED
**Analytic Model with Minimal State Dimension**

\[ P(t) = P(t)Q(t), \quad P(0) = I \]

And \( Q \) is given by

\[
\begin{bmatrix}
6\lambda_1 - 2\lambda_2 & 6\lambda_1 C_{11} + 2\lambda_2 C_{12} & 0 & 0 \\
-10\lambda_1 - 1\lambda_2 & 1\lambda_2 C_{11} + 2\lambda_2 C_{12} + 6\lambda_1 C_{21} + 2\lambda_2 C_{22} & 0 & 0 \\
0 & 0 & -12\lambda_1 - 6\lambda_2 & 2\lambda_2 C_{23} + 4\lambda_2 C_{24} + 6\lambda_1 C_{32} + 2\lambda_2 C_{33} \\
0 & 0 & 0 & -18\lambda_1 - 8\lambda_2 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}
\]

The above results in the same simple formula

\[ P_f = [P(t)]_{(1,7)} \approx [Q]_{(1,7)} t = 6\lambda_1 [1 - C_{01}] t + 2\lambda_2 [1 - C_{02}] t, \quad t \leq t_m \]
• KEY TO ENHANCED RELIABILITY—HIGH COVERAGE
  ○ CURRENTLY ACHIEVABLE VALUE IN FTFCS?
    — $1 - C_{01} \approx 10^{-1}$
  ○ IMPROVEMENT DESIRABLE?
    — REDUCTION OF $1 - C_{01}$ BY SEVERAL ORDERS OF MAGNITUDE
  ○ ADEQUATE VALUE?
    — $1 - C_{01} \approx n^2 \lambda_{in}$
  ○ WHEN THE ABOVE IS ACHIEVED
    — SURE IS NEEDED FOR ACCURACY
    — ASSIST IS NEEDED FOR MODELING
  ○ A BY-PRODUCT OF ASSIST
    — TRANSITION RATE MATRIX OF A MARKOV PROCESS

REFERENCES


