RELIABILITY ASSESSMENT OF RECONFIGURABLE FLIGHT CONTROL SYSTEMS USING SURE AND ASSIST 1

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

1 Support by the NASA under Cooperative Agreement NCC-1-336, and by the ASEE Summer Faculty Fellowship is acknowledged.

Thanks to Ricky Butler and Allan White for their time and insightful suggestions.
• SOME BACKGROUND

○ MARKOV PROCESS[7]:

\{X(t) \mid t \in (0, \infty)\} IS A MARKOV PROCESS IF \( \forall t_0 < t_1 < \cdots < t_n < t \), THE CONDITIONAL DISTRIBUTION OF \( X(t) \) FOR GIVEN VALUES OF \( X(t_0), \ldots, X(t_n) \) DEPENDS ONLY ON \( X(t_n) \)

\[ P(X(t) \leq x \mid X(t_n) = x_n, \ldots, X(t_0) = x_0) = P(X(t) \leq x \mid X(t_n) = x_n) \]

* 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

\[ \Rightarrow \]

\[ F(t) \ (\text{TIME A PROCESS SPENDS IN A STATE}) \text{ IS EXPONENTIAL} \]

\[ P(T \leq t) = F(t) = 1 - e^{-F(0)t} \]

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

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

[Diagram of subsystems in the FTFCS]

Functional dependency of subsystems in the FTFCS

○ A PARALLEL-TO-SERIES INTERCONNECTION OF 5 BLOCKS

* FLIGHT CRITICAL PROCESSORS

—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

\[ 1 - e^{-\lambda t} \leq F(t) \leq 1 - e^{-\lambda t}, \quad t \leq t_m \]

- 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

- BLOCK FAILURE PROBABILITY BOUNDS

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

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

• BLOCK FAILURE PROBABILITY BOUNDS

λ = 10^{-5}

μ = 10^{-1}

σ = 10^{-2}

C_{01} ∈ [0.99, 1.0]

C_{12} ∈ [0.95, 1.0]

C_{23} ∈ [0.90, 1.0]

τ = 1

• 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

λ = 10^{-5}

μ = 0.9

C_{01} ∈ [0.99, 1.0]

C_{12} ∈ [0.95, 1.0]

C_{23} ∈ [0.90, 1.0]

τ = 1
• EFFECTS OF NEGLECTING REMOVAL TIMES

○ BLOCK FAILURE PROBABILITY BOUNDS

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

○ BLOCK FAILURE PROBABILITY

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

• FURTHER SIMPLIFICATION OF THE PROCESSOR MODEL

○ A SYSTEM WITH AN EQUIVALENT FIRST ORDER EFFECT

○ VALID IF RELATIVE TO THE FAILURE PROCESS
- REMOVAL OF FAULTY SUBSYSTEMS IS FAST
- MISSION TIME IS SHORT
JUSTIFICATION OF 2ND APPROXIMATION

- AN T+1 STATE MARKOV PROCESS

- COMBINATORY APPROACH

FAILURE OF AN T-SUBSYSTEM BLOCK
- OR MORE FAILED SUBSYSTEMS, OR
- INCORRECT RECONFIGURATION DECISION

SOME NOTATIONS
- failure rate of a subsystem
- transition probability
- coverage of a transition
- mission time
- transition time
- $p_i(t)$: transition probability
- $C_i$: coverage of a transition

FAILURE RATE OF A SUBSYSTEM

where

$\lambda_i = \sum_{j=1}^{i} \lambda_j$

$P_i(t) = \begin{cases} 1 - e^{-\lambda_i t} & \text{if } i = 0 \\ 0 & \text{otherwise} \end{cases}$
AN ALTERNATIVE WHEN \( Q \) IS KNOWN

\[
P(t) = P(t)Q(t)
\]

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

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

\[
P(t) = e^{Qt}
\]

\[
= P^N \left(\frac{t}{N}\right)
\]

\[
\approx (I + Q \frac{t}{N})^N, \quad \text{EULER APPROXIMATION}
\]

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

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

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

\[
= [1 - C_{[0]}] n \lambda t_m
\]
**APPROXIMATION ERROR**

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

**DEFINE THE APPROXIMATION ERROR**

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

**THEN**

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

**NOTE THAT**

\[
\sum_{i=2}^{N} \frac{1}{i!} |(Qt)^i|_{1,r+1} \leq (i + 1)/(n\lambda t)^i
\]

**THEREFORE**

\[
|e| \leq \lim_{N \to \infty} \sum_{i=2}^{N} \frac{1}{i!} |(r + 1)(n\lambda t)^i|
\]

\[
\leq \frac{(r + 1)(n\lambda t)^2}{2} \lim_{N \to \infty} \sum_{i=0}^{N-2} \frac{n\lambda t}{2^i}
\]

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

\[
< (r + 1)(n\lambda t)^2 , \quad n\lambda t < 1
\]

**SOME REMARKS**

- **GOOD APPROXIMATION**

\[
(r + 1)(n\lambda t)^2 \ll (1 - C_{b1})n\lambda t
\]

\[
C_{b1} < 1 - n^2\lambda t
\]

- **REDUNDANT SYSTEM VERSUS SIMPLE SYSTEM**

\[
|1 - C_{b1}|n\lambda t_m < \lambda t_m
\]

\[
C_{b1} > 1 - \frac{1}{n}
\]

- **IN GENERAL, 1 - C_{b1}** decreases as \( n \) increases

⇒ THERE IS AN \( n \) AT WHICH

\[
m_{\text{min}}(1 - C_{b1})n\lambda t_m
\]

**IS ACHIEVED**

- **EXAMPLE**

**REDUNDANCY MANAGEMENT**

<table>
<thead>
<tr>
<th>( n )</th>
<th>( C_{b1} )</th>
<th>( (1 - C_{b1})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  

\[ \sum (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

\[ \sum (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

\[ \sum (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

○ HIGHER RATES TO DEATH STATES  

\[ - C_{i+1} \leftarrow 1, F_i(t) \leftarrow 1 \]

\[ (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

\[ (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

\[ (0^i - (1)^i - (\lambda t)^i) \sum (0^j - (1)^j) \]

○ GOOD APPROXIMATION  

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

\[ (1 - C_{i+1})4\lambda t \gg (4\lambda t)^2 \leftrightarrow C_{i+1} \ll 1 - 4\lambda t \]

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

\[ (1 - C_{i+1})4\lambda t \gg (4\lambda t)^2 \leftrightarrow C_{i+1} \ll 1 - 4\lambda t \]

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

\[ (1 - C_{i+1})4\lambda t \gg (4\lambda t)^2 \leftrightarrow C_{i+1} \ll 1 - 4\lambda t \]

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

\[ (1 - C_{i+1})4\lambda t \gg (4\lambda t)^2 \leftrightarrow C_{i+1} \ll 1 - 4\lambda t \]
• ANALYSIS OF THE EFFECTOR BLOCK

1. C/E means computer/effectuator 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

○ A SIMPLE CASE STUDY

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

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

\[ C_{01}^0 \in [0.99, 1.0] \]
\[ C_{12}^1 \in [0.95, 1.0] \]
\[ C_{23}^2 \in [0.90, 1.0] \]
\[ C_{01}^2 \in [0.99, 1.0] \]

○ 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

\[ P_f = 6\lambda_1|1 - C_{01}^1|t + 2\lambda_2|1 - C_{01}^2|t, \quad t \leq t_m \]
STATE TRANSITION DIAGRAM

USING ASSIST AND SURE

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

\[
\begin{pmatrix}
-6\lambda_1 - 2\lambda_2 & 6\lambda_1 C_{01} + 2\lambda_2 C_{02} \\
-12\lambda_1 - 6\lambda_2 & 12\lambda_1 C_{11} + 2\lambda_2 C_{12} + 6\lambda_1 C_{20} \end{pmatrix}
\]

THE ABOVE RESULTS IN THE SAME SIMPLE FORMULA

\[ P_f = [P(t)]_{11(t)} \approx \mathbb{E}[Q]_{11} = 6\lambda_1[|1 - C_{01}|t + 2\lambda_2|1 - C_{02}|_2], \quad t \leq t_m \]
• 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


