Outline

- Fault Tolerant Techniques
- Timeline
  - Beginning research
  - Beginning implementations
  - Dynamic error detection/correction
  - Fault tolerance today

N-Version Software Techniques

- N-Version Programming
  - Run multiple versions of software and vote
- Recovery Blocks
  - Acceptance Test
  - Restore system state and retry

Fault Tolerance Proposal & Initial Research

- NATO
- '68-'69 NATO
- '66 IEEE Reliable Automata Conf
- '74 RB proposed
- '76 RB implemented, NVP proposed
- '78 NVP implemented
- '78 NVP Common Mode Failures, Navy RB Implementation
- '85 NVP Comparison Problems
- '85 NVP
- '85 Hardware Recovery Cache
- '85 ELEKTRA railway
- '84 Boeing 777
- '85 SACEM subway control
- '86 ABFT Simplex Arch
- '87 0(n-1) VP
- '88 IEC 61508
- '89 NVP
- '91 NVP Weighting
- '92 ABFT
- '93 NVP
- '94 Boeing 777
- '95 ELEKTRA railway
- '96 ABFT Simplex Arch
- '97 0(n-1) VP
- '98 ELEKTRA railway
- '99 Boeing 777
- '00 IEC 61508
- '01 NVP Weighting
1960s: SW Fault Tolerance Proposed

- Problem recognized: “The Software Crisis”
- Acknowledgement that software will have bugs
- Many discussions of problem
  - ’66: IEEE Reliable Automata Conference
  - ’68-’69: NATO

1970s: Initial Research

- Recovery Blocks
  - ’74: proposed
  - ’76: first implementation
    - Successful, detected intentional and accidental faults
- N-Version Programming
  - ’76: proposed
  - ’78: first implementation, Chen & Avizienis paper
    - Semi-successful
    - Raised many development questions

Initial Implementations & Limitations

- ’78: Pascal adds “ENSURE” statement for acceptance test
- ’80: Built HW recovery cache, restores state faster than SW cache
- ’85: Navy controls used RBs

Early 80s: Beginning Implementations

- ’78: SACEM subway control
- ’80: IEC 61508
- ’85 ABFT
- ’90: Boeing 777
- ’94: Simplex Architecture
- ’95: ELEKTRA railway
- ’96: ABFT Simplex Architecture
- ’97: t/(n-1) VP
- ’98: NVP Comparison Problems
- ’99: 60-80 NVP implementation
- ’00: 98 IEC 61508
- ’01: NVP Weighting
- 2010: NVP Weighting
1980s: Limitations

- Problems found in NVP
  - Common mode failures
  - Comparison of floating point numbers
  - Comparison at values where behavior changes – “cross-over points”

1990s: Dynamic Error Detection

- Acknowledgement that specifications will have bugs
- ABFT (Algorithm Based Fault Tolerance) based on control system algorithms
- Find source of errors during operation
- Allows ability to rewrite problem areas

1990s & 2000s: Dynamic Error Correction

- ’96: Simplex Architecture
  - Switch to simpler, less efficient algorithm
  - Online upgrades
- ’01: Weighted voting
  - Grosspietsch & Romanovsky paper
‘98: Safety standard IEC 61508
– Functional safety of E/E/PE safety-related systems

<table>
<thead>
<tr>
<th>Year</th>
<th>System</th>
<th>Faults Tolerated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mid 80s</td>
<td>SACEM subway speed control</td>
<td>HW design, compiler</td>
</tr>
<tr>
<td>1987</td>
<td>Airbus flight control</td>
<td>SW design</td>
</tr>
<tr>
<td>1994</td>
<td>Boeing 777</td>
<td>HW design, compiler</td>
</tr>
</tbody>
</table>

Questions?