Arquiteturas tolerantes a falhas

Alta disponibilidade e ultra dependabilidade

Taisy Silva Weber
UFRGS

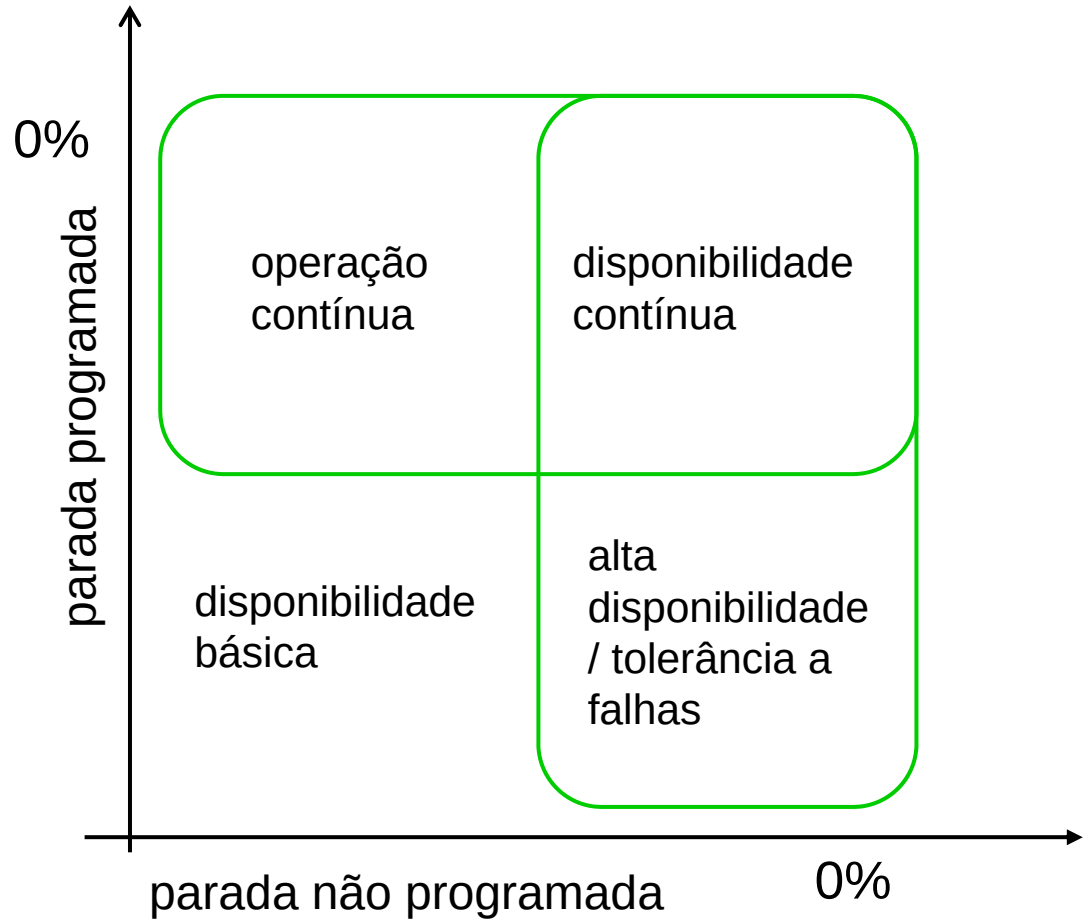
Arquiteturas para alta disponibilidade

- alta disponibilidade
  - possível intervalos pequenos para reparo
- importante
  - redução do MTTR
- áreas de aplicação
  - sistemas de transação
  - redes
  - telefonia
- medidas usuais
  - 7 x 24 (operação contínua)
  - 5 noves (uptime)

99,999 %

sistemas usados em aplicações em que falhas podem provocar enormes prejuízos financeiros como transações bancárias, bolsas de valores, reservas aéreas, e-comerce, transações on-line, ...

disponibilidade: alta X contínua



alta disponibilidade, disponibilidade contínua e tolerância a falhas podem aparecer como sinônimos, mas alguns autores fazem distinção

Wendy Bartlett e Lisa Spainhower. Commercial Fault Tolerance: **A Tale of Two Systems**, IEEE TRANS. ON DEPENDABLE AND SECURE COMPUTING, Jan-Mar 2004.

disponibilidade: alta X contínua

Availability Level		Average Yearly Downtime
Conventional	0,99	87 hours, 40 minutes
High Availability	0,999	8 hours, 46 minutes
	0,9995	4 hours, 23 minutes
	0,9999	52 minutes, 36 seconds
Continuous Availability	0,99999	5 minutes, 16 seconds
	0,999999	31.6 seconds

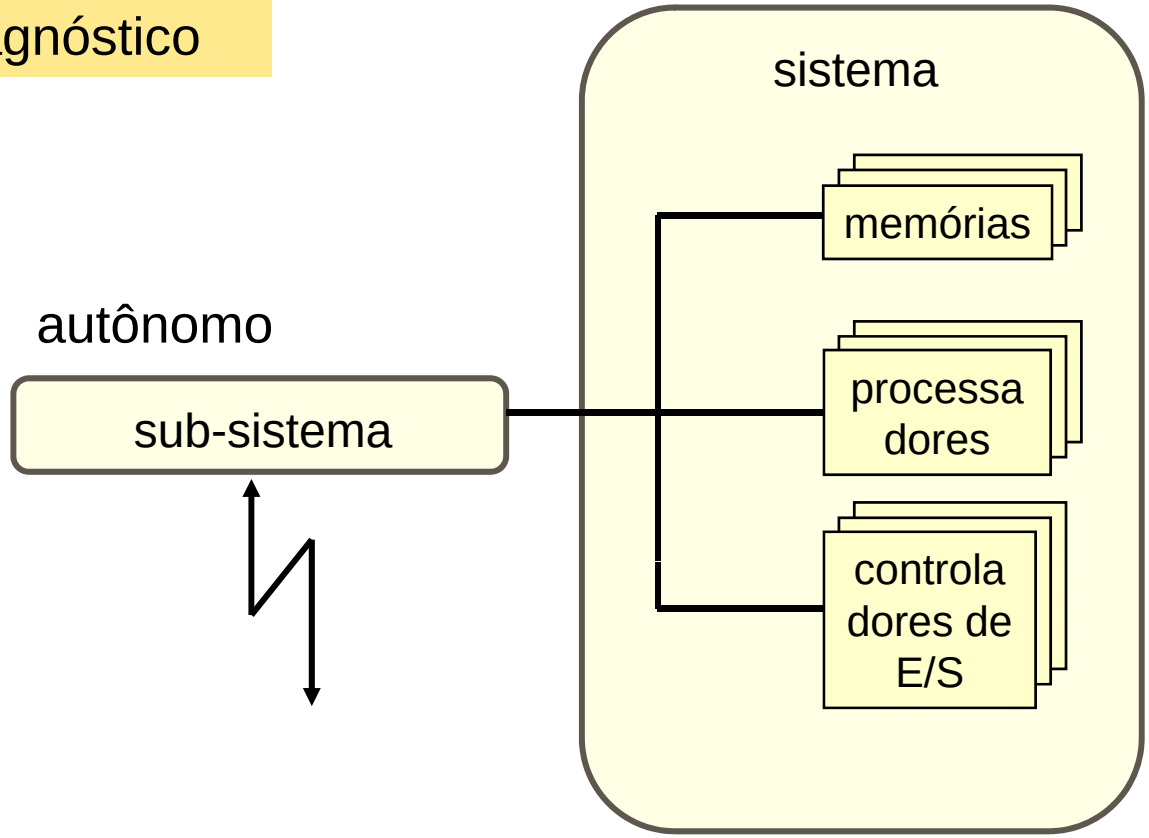
http://www.stratus.com/About/UptimeMeter.aspx

sub-sistema de manutenção

supervisão, detecção e diagnóstico

não pode ser o componente menos confiável do sistema

não dispensa outras técnicas de TF: códigos de correção e detecção de erros; recuperação de erros transitórios

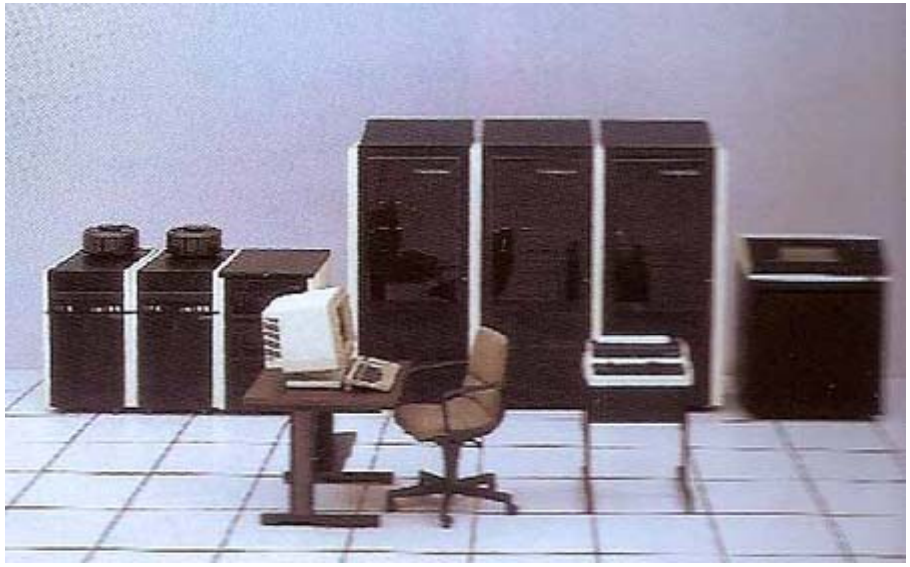


Sistemas comerciais

- tolerantes a falha
  - computadores de grande porte específicos para aplicações comerciais tolerantes a falhas (sistemas de transações)
- exemplos:
  - Tandem: fundada em 1976
    - mecanismos de TF implementados em software
  - Stratus: fundada em 1980
    - mecanismos de TF implementados em hardware

técnicas ainda usadas para servidores e computadores de alta disponibilidade

NonStop computers

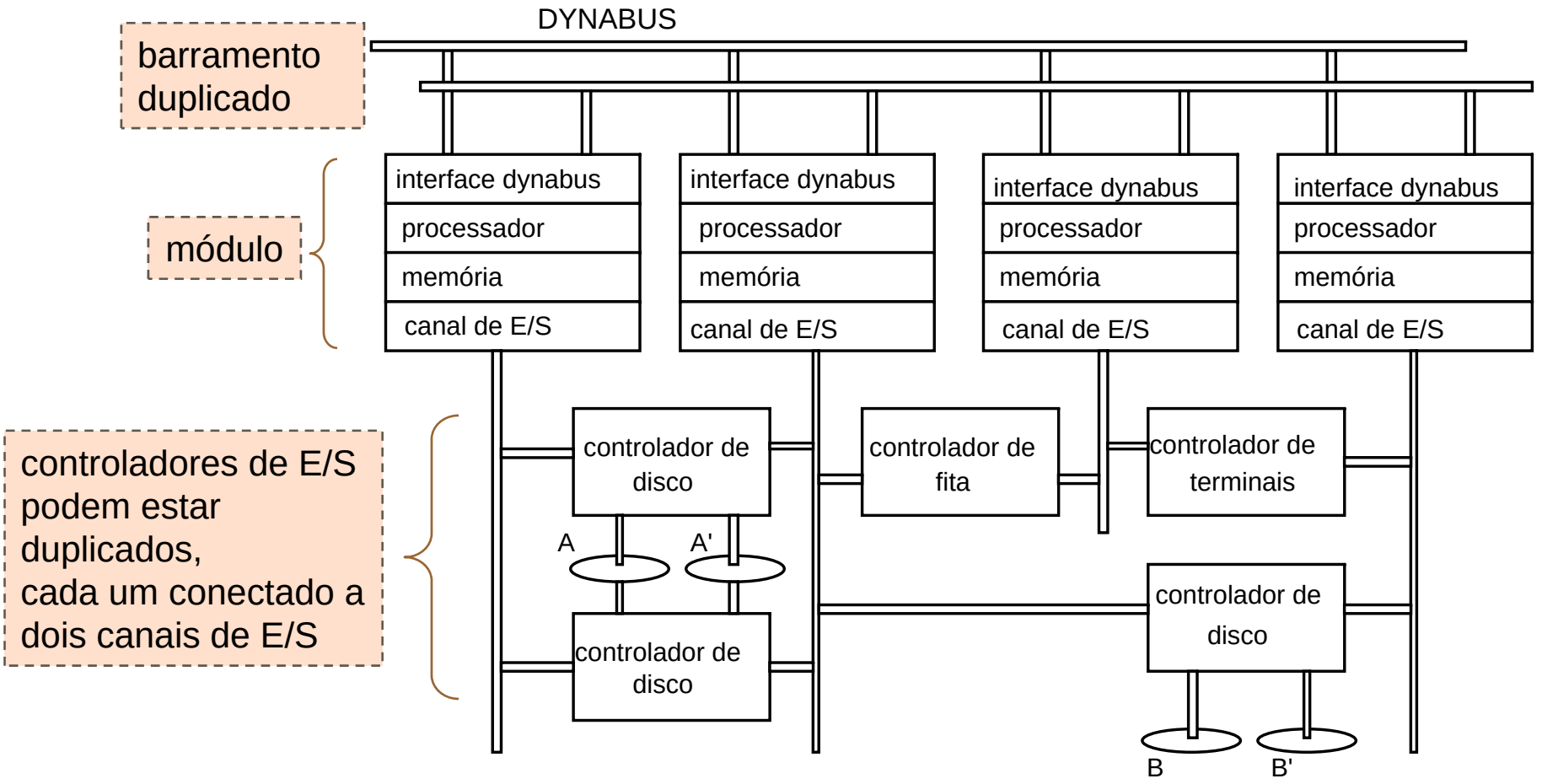


Tandem

HP

Tandem NonStop

primeiro sistema comercial modular e escalável projetado especificamente para disponibilidade contínua

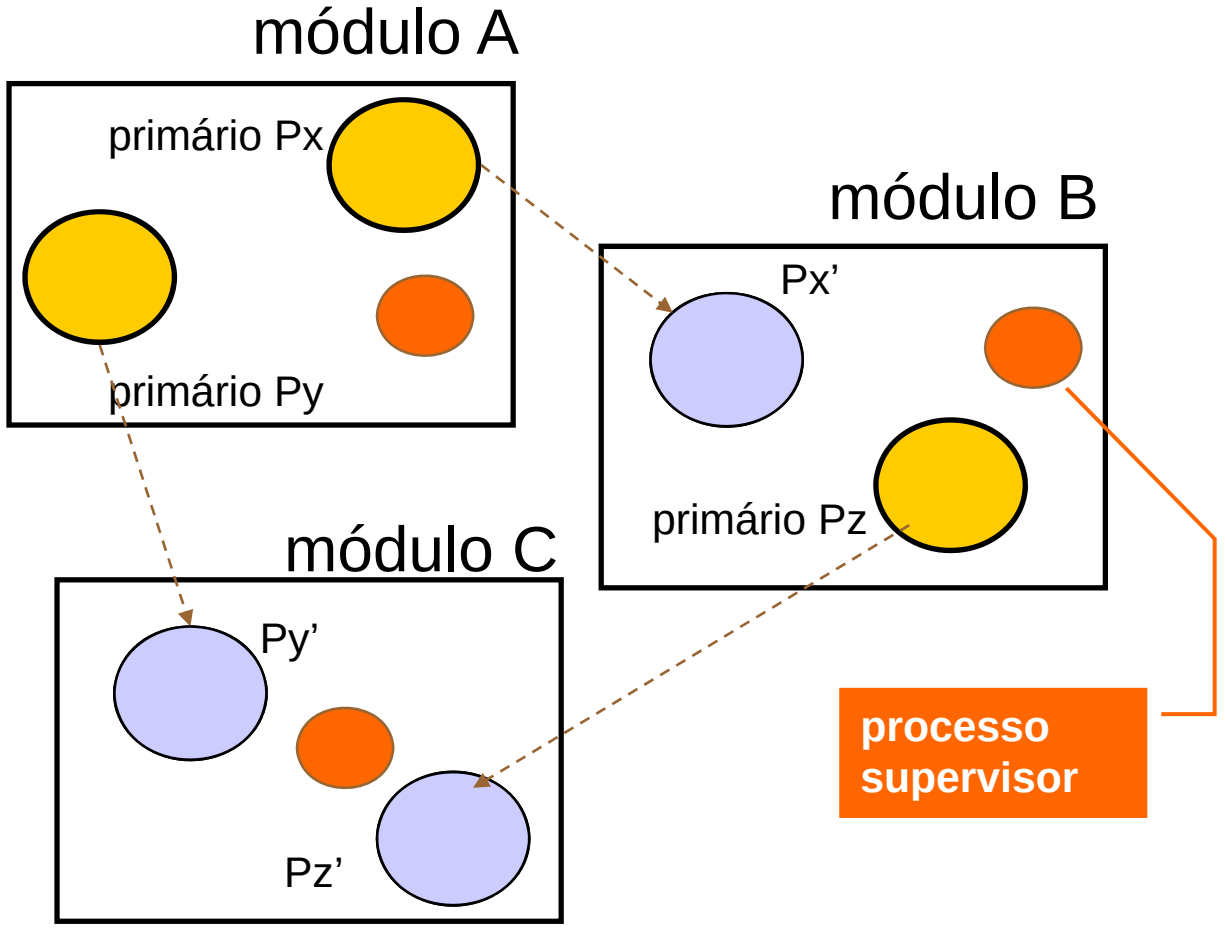


Primários e backups

redundância dinâmica em software

pares para processos do sistema e do usuário: processo primário ativo & processo substituto passivo (backup)

primário envia pontos de recuperação para o backup



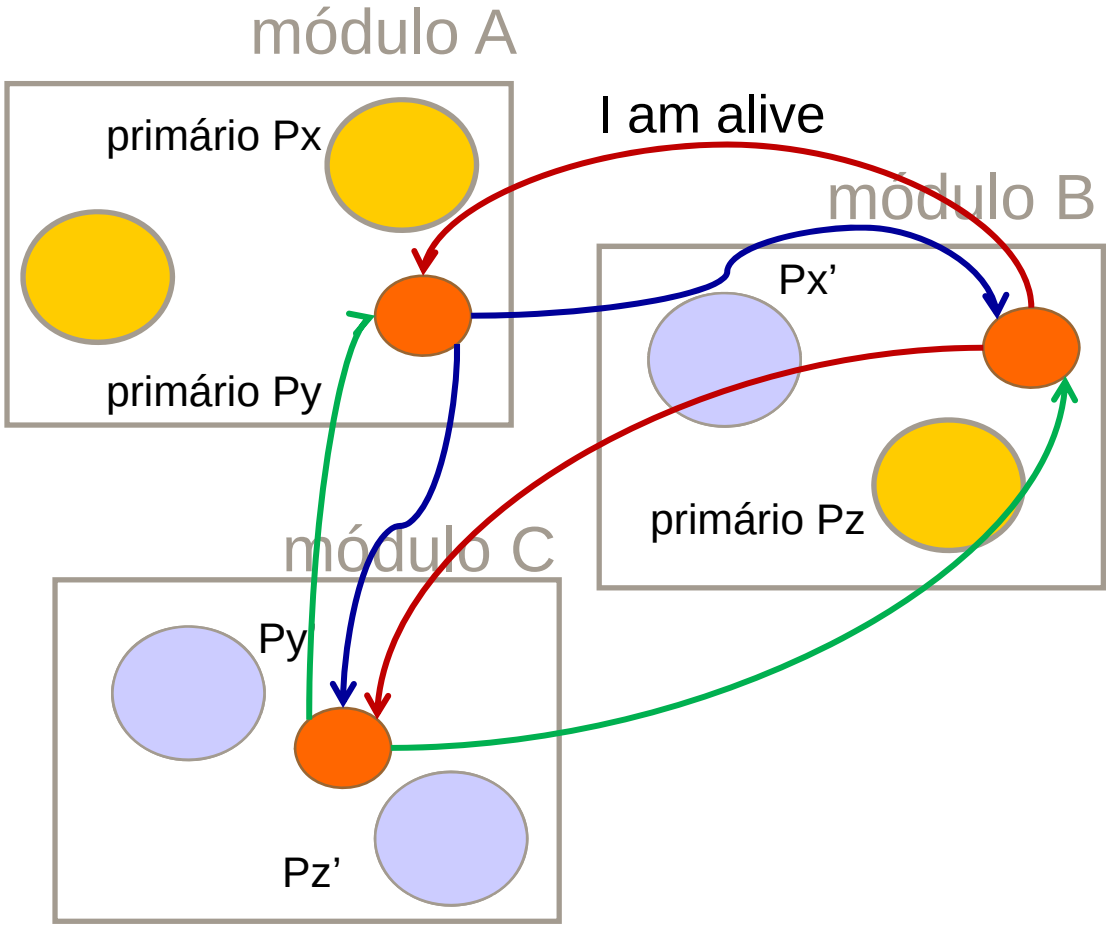
Detecção

assumido *fail-stop*

a cada 1 s: cada supervisor envia sinal de vida a todos os outros módulos

a cada 2 s: supervisor verifica sinal dos outros módulos

falta de um sinal: módulo falhou



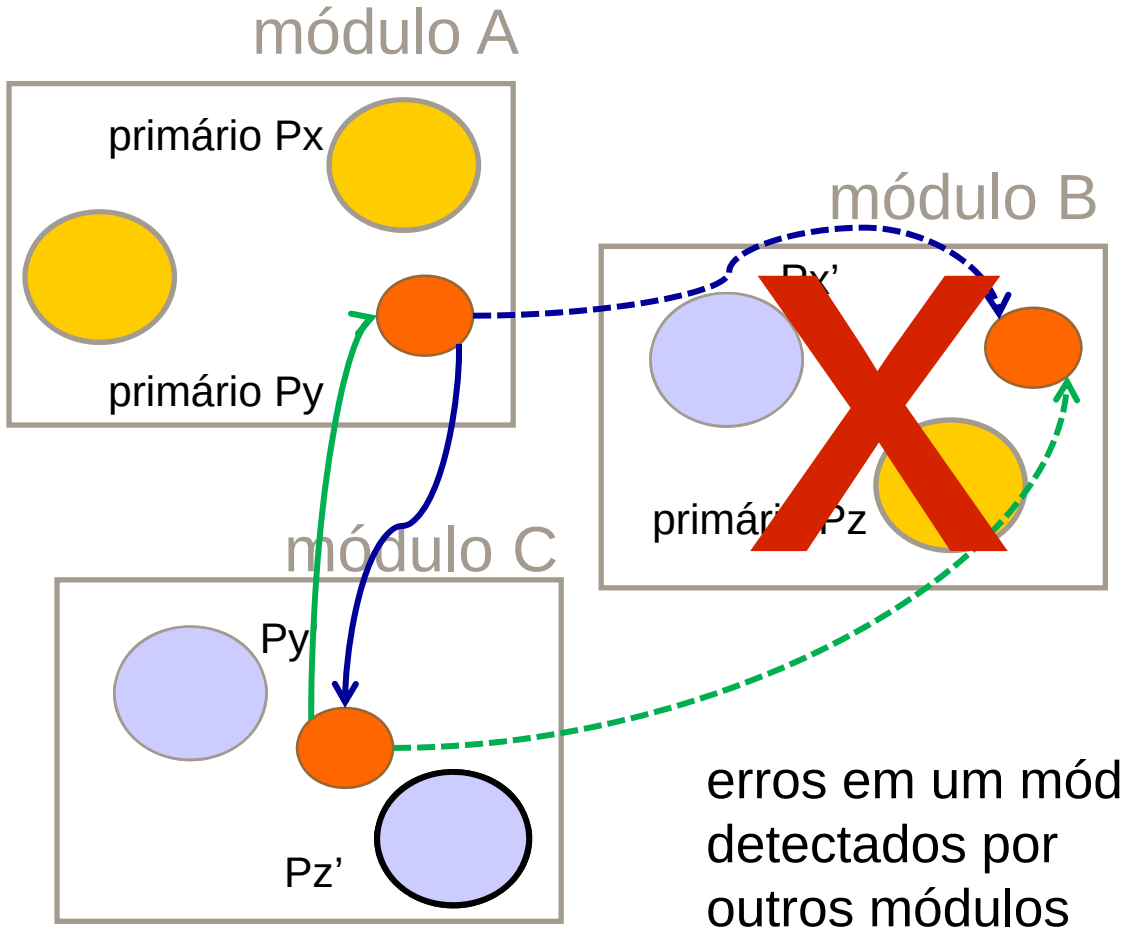
Detecção

assumido *fail-stop*

módulo B parou

supervisores de A e C não recebem sinal de B

supervisores de A e C concluem que B falhou



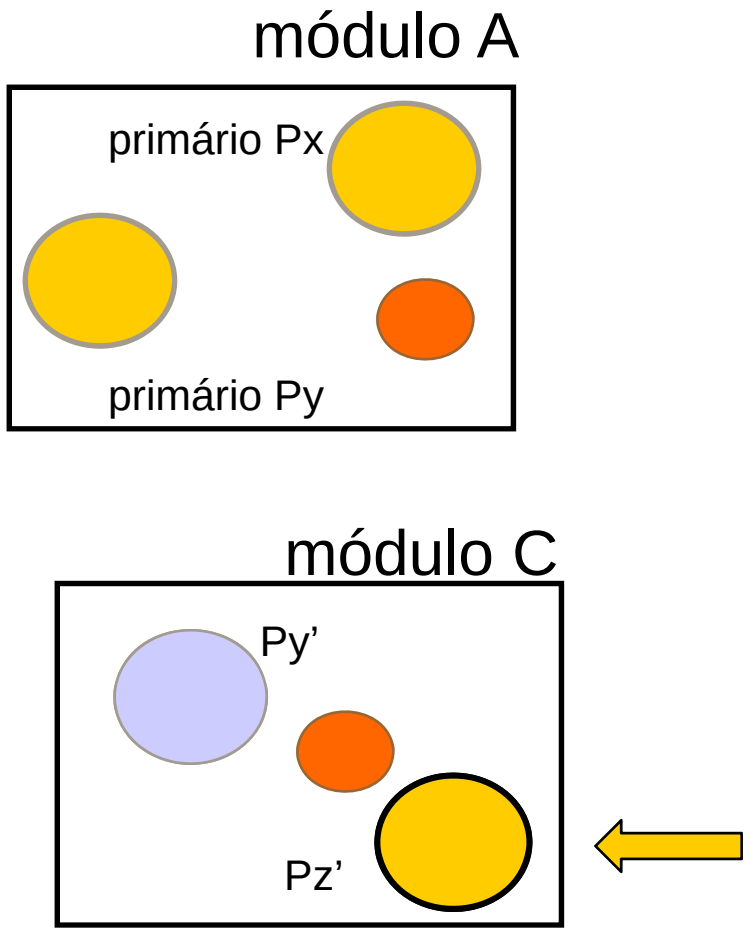
erros em um módulo detectados por outros módulos

Tandem: detecção e recuperação

- operações de entrada e saída
  - detecção por time-out

    processo de E/S substituto entra em operação

- recuperação
  - processos backup rolam para o último PR e são ativados como primários
  - sistema é reconfigurado
    - após reparo do módulo novos primários criam substitutos no módulo



Stratus

modelos atuais (2010)

Continuum Series

Stratus® ftServer® 4300 System

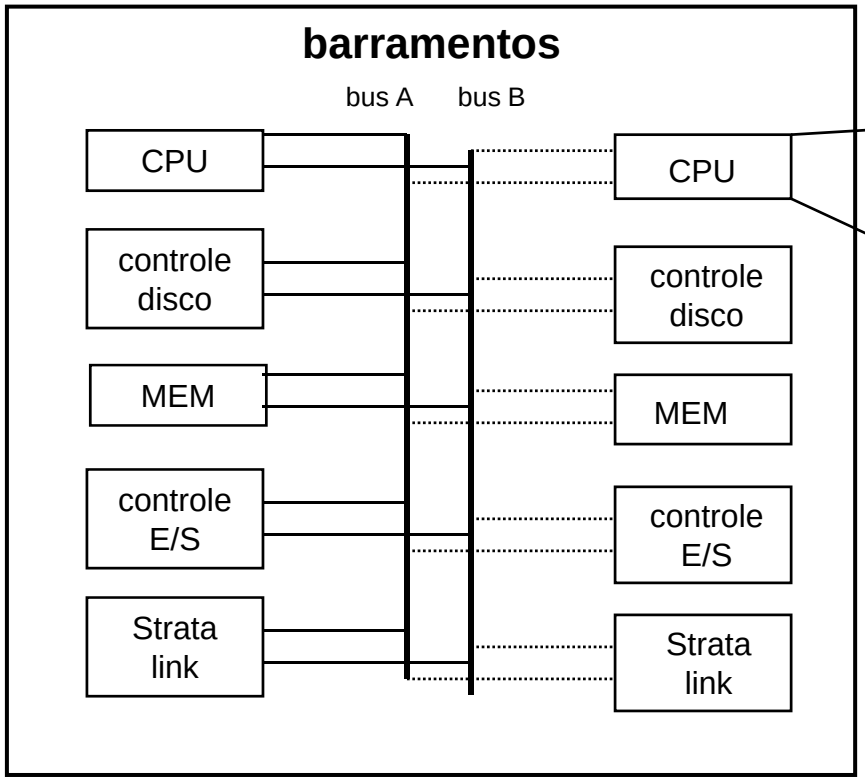
Stratus Technologies

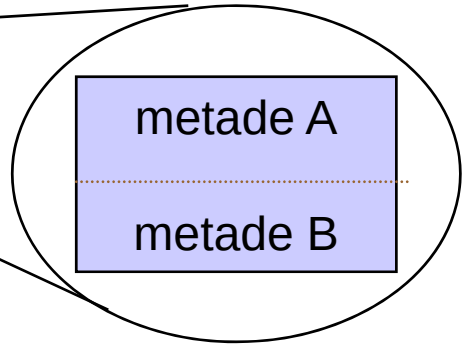
TOTAL AVAILABILITY

abordagem pair-and-spare

Stratus

CPU e memória com componentes duplicados com comparador (redundância estática)





XA/R Series 300
modelo antigo

módulo com 2 boards

módulos em rede local (Strata Link)

Servidores HA

- fornecedores atuais de soluções para servidores de alta disponibilidade
  - Sun (oracle)
  - Dell
  - HP
  - IBM
  - Stratus
- evtl outros fabricantes
  - Bull
  - Fujitsu
  - Hitashi

pesquisar no site dos fabricantes para descobrir modelos, características, técnicas de TF empregadas e custo

http://www.stratus.com/About/UptimeMeter.aspx

Servidores

- reconfiguração automática
  - reinicia imediatamente após defeito, isolando automaticamente o componente falho
  - testa os componentes do sistema
    - a cada vez que o equipamento é ligado
    - ou quando é gerada uma interrupção externa
- fontes de energia e ventilação redundantes
- monitoramento ambiental
  - proteção contra temperaturas extremas, falta de fluxo de ar ou flutuações de energia

Servidores

- códigos de detecção e correção de erros
- ferramentas de monitoramento
  - registradores para monitorar o sistema e implementar *cão de guarda*
  - acesso por software especial para extrair dados sobre desempenho e para a manutenção
- ferramentas de diagnóstico *online*
- *hot swap*
  - troca de componentes com o sistema em operação

módulos de energia/ventilação, placas de CPU/memória e de I/O

Sistemas de telefonia

- electronic switching systems (ESS)
  - técnica usual: duplicação e comparação

antigamente eram classificados como críticos, hoje ESS são geralmente classificados como HA ou disponibilidade contínua

sistemas de telefonia são mais antigos que sistemas de computação

início: 1878

Sistemas críticos

ultra dependabilidade

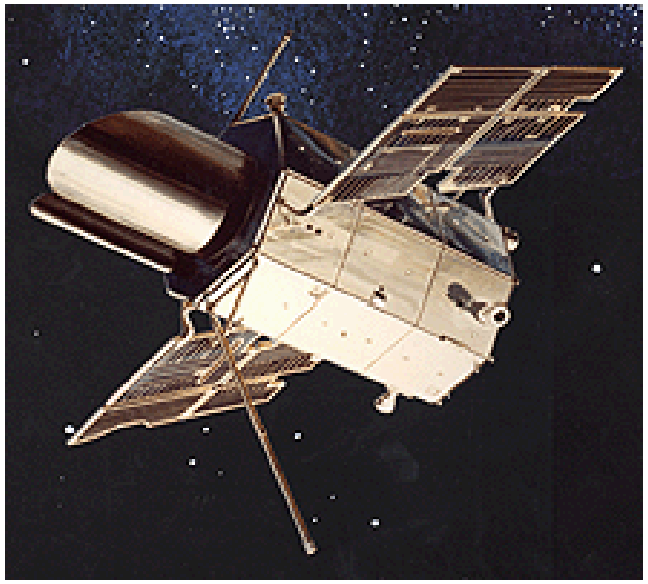
alta dependabilidade

- primeira área de computadores TF
- controle de aeronaves e satélites
- exemplos: início década de 60
  - satélite OAO
    - (Orbiting Astronomical Observatory)
    - um dos últimos computadores construídos com componentes discretos
  - Apollo
    - TMR para processadores
    - espelhamento de memória e ECC 1963 - 1972

Satélites

OAO - 1

lançado em 8 de abril de 1966;
funcionou perfeitamente durante 77 minutos;
defeito foi atribuído a falha no sistema de potência (fonte)



OAO - 3

Agosto de 1972 a Fevereiro de 1981 (9.5 anos)

Fly-by-wire control systems

na NASA,o primeiro avião *fly-by-wire* foi o F-8C Crusader (em 1972)

o A320 foi o primeiro avião comercial *fly-by-wire* digital (em serviço: 1988)

cabine de um airbus A321
(projeto 1989 – primeiro vôo 1993)

Airbus fly-by-wire: A total approach to dependability. P Traverse, I Lacaze, J Souyris - Building the Information Society, 2004 - Springer

Computadores de bordo

ultra dependabilidade

aplicação crítica de tempo real

Fly-by-wire control systems

- ✓ controle de aeronaves

perda de controle de poucos milisegundos pode ser fatal

  - ✓ tempo real
    - ✓ com tempo de atuação curto
    - ✓ interrupção no funcionamento: inadmissível
  - ✓ reparo:
    - ✓ possível apenas durante os intervalos de vôo
  - ✓ confiabilidade:
    - ✓ da ordem de 10^{-9} ou 10^{-10} falhas por hora para um vôo de 10 horas

1,14 milhões de anos de operação

FTMP e SIFT

dois computadores desenvolvidos a partir da mesma especificação

- ✓ década de 70 (NASA)
  - ✓ redundância modular tripla (TMR)
- ✓ FTMP
  - ✓ Fault Tolerant Multi-Processor
- ✓ SIFT
  - ✓ Software Implemented Fault Tolerance

SRI International, 1972

- ✓ votador implementado em hardware,
- ✓ todos processadores sincronizados
- ✓ relógio central é tolerante a falhas

- ✓ votação por software,
- ✓ processadores são assíncronos,
- ✓ não há relógio central
  - ✓ sincronização de resultados para votação garantido por software

SIEWIOREK, D. Architecture of fault-tolerante computers, cap 2. **Fault-Tolerant System Design**. Prentice Hall, New Jersey, 1996

FTMP

- 5 barramentos redundantes
  - processadores e módulos de memória ligados ao sistema de barramento por interfaces especiais

BGs - bus guardians

- tríade = 3 processadores + 3 memórias
  - elementos da tríade executam a mesma tarefa e comunicam-se através de 3 dos 5 barramentos
    - BGs votam sobre dados da tríade colocados nos 3 barramentos
  - falha mascarada em processador, memória ou barramento

FTMP

- tríades diferentes executam tarefas diferentes
- processadores e módulos de memória estepe
  - objetivo:
    - substituir um elemento de uma tríade que falhou
- distribuição dinâmica de tarefas entre as tríades
  - objetivo:
    - reconhecer falhas nos votadores
- reconfiguração periódica
  - objetivo:
    - reconhecer falhas no mecanismo de reconfiguração

SIFT

- módulos processadores interligados por barramento redundante
  - processadores operam assincronamente em relação aos demais
  - sincronização de resultados para votação por software
  - uma tarefa é alocada sempre a 3 módulos:
    - cada módulo envia seu resultado aos outros 2 usando o barramento redundante
    - cada módulo realiza votação majoritária por software

votação majoritária: (2-em-3)

Comparação FTMP e SIFT

- ambos com alta confiabilidade para aplicações críticas tempo-real
- FTMP:
  - esquema de votação mais eficiente (hardware)
  - tolerância a falhas não é visível a partir da aplicação
- SIFT:
  - esquema de votação em software
    - mais versátil
    - elimina necessidade de clock tolerante a falhas
  - tolerância a falhas é visível a partir da aplicação

Space Shuttle

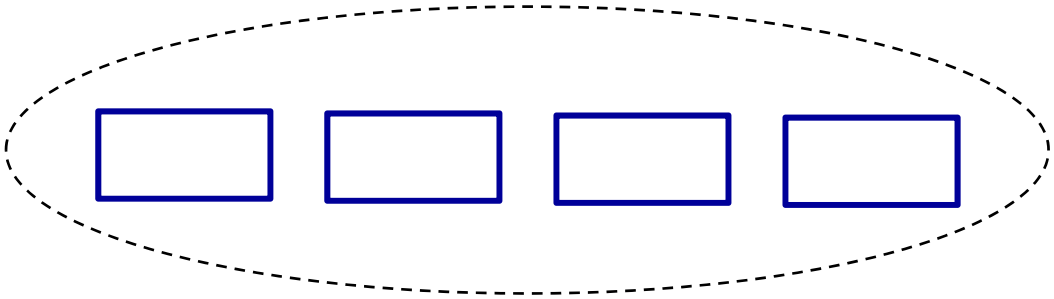
primeiro vôo: 13/04/1981

últimos vôos: 2011

Columbia †
Challenger †
Discovery
Atlantis
Endeavour

Computers in Spaceflight: The NASA Experience (James E. Tomayko - 1987)
Chapter Four - -Computers in the Space Shuttle Avionics System
http://www.hq.nasa.gov/office/pao/History/computers/Ch4-4.html

Space Shuttle computer



4 computadores atuam nas fases críticas
mascaramento NMR
detecção cruzada (cada computador ouve todos os demais)

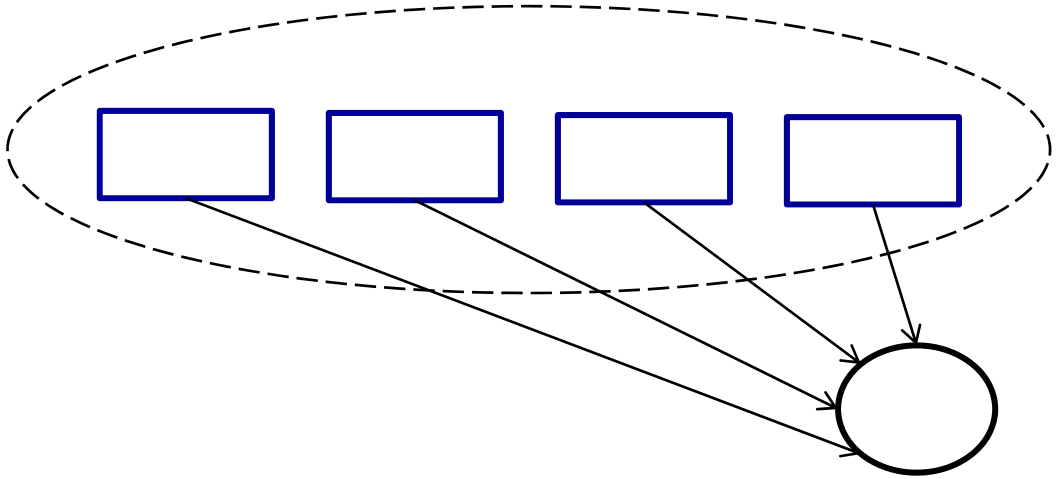
quinto computador realiza operações não críticas, atua como backup dos demais,
software diversitário

suporta até duas falhas

abordagem semelhante a SIFT (1976)

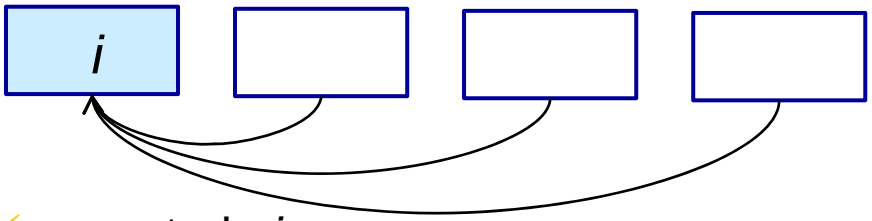
software primário é da IBM, o diversitário da Rockwell

Space Shuttle: operação

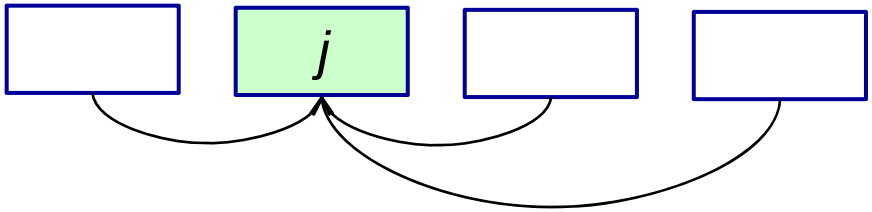


- mascaramento
  - saídas são votadas nos atuadores

Space Shuttle: detecção de falha



- para todo *i*
  - *i* escuta as saídas dos demais
  - *i* compara com suas saídas (por software)
  - se *i* detectar desacordo: avisa o computador suspeito j



- em cada computador *j*
  - sinais de desacordo recebidos por *j* são votados em um circuito especial (gerente de redundância)
  - se o voto for positivo, o suspeito *j* é desativado

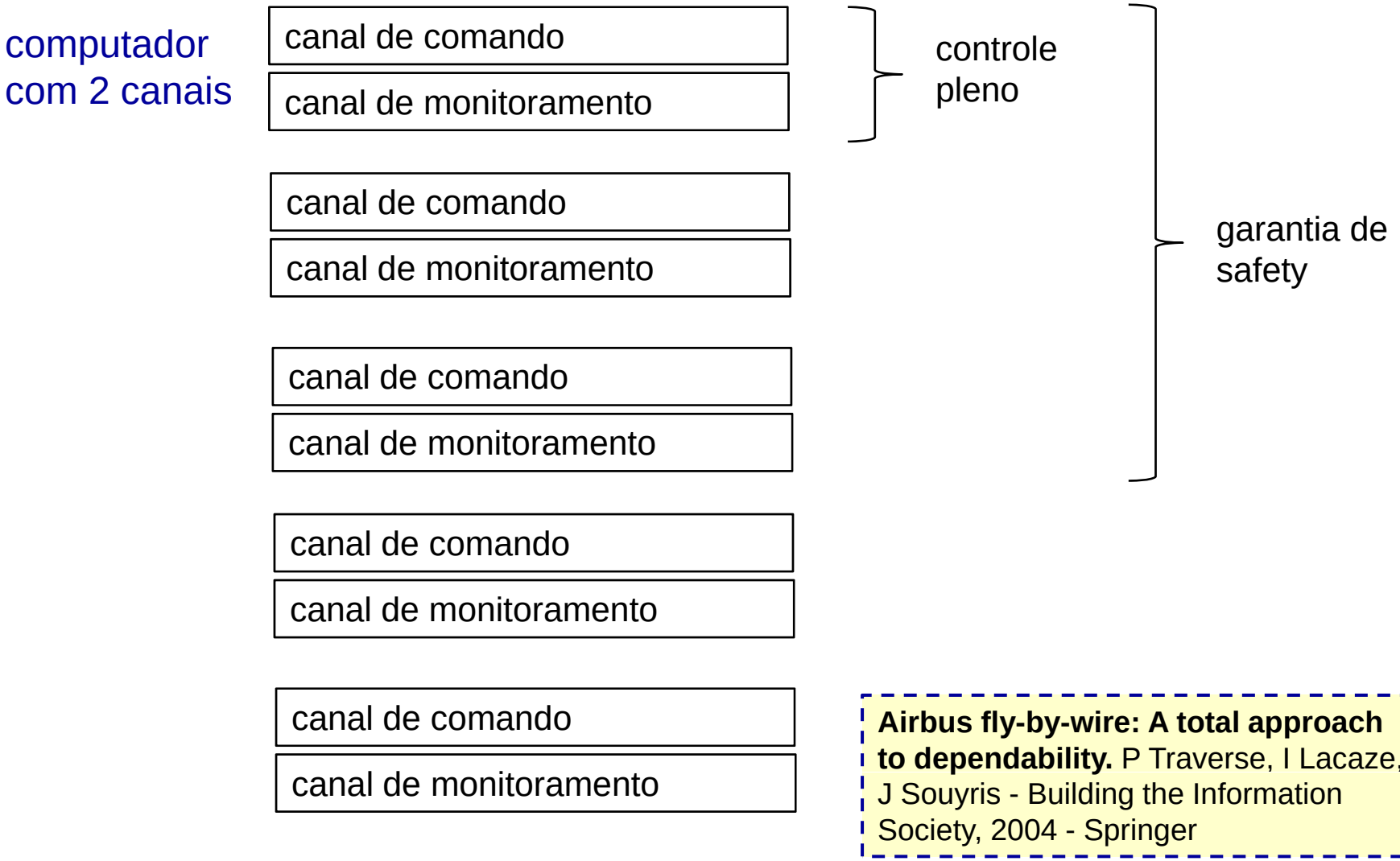
Airbus

- controle de superfícies de vôo
  - controle elétrico, ativação hidráulica
    - A320/A330/A340
    - A340 entrou em operação em 2002
  - controle elétrico, ativação elétrica (*power-by-wire*)
    - A380, A400M
- cada computador: canal de comando e canal de monitoramento
  - cada canal é diferente (diverso) em hardware e software
- 5 computadores
  - cada um capaz de pleno controle da aeronave, 3 seriam suficientes para atender safety
- microprocessadores COTS

RTCA

norma DO 178B - nível A (software)

Airbus



Airbus fly-by-wire: A total approach to dependability. P Traverse, I Lacaze, J Souyris - Building the Information Society, 2004 - Springer

Bibliografia

- capítulos de livros
  - SIEWIOREK, D. Architecture of fault-tolerante computers, cap 2. **Fault-Tolerant System Design**. Prentice Hall, New Jersey, 1996
- artigos
  - AVIZIENIS, A. **Fault Tolerance Infrastructure for Dependable Computing with High-Performance COTS Components**. DSN, IEEE 2000
  - Cristian Constantinescu, **Trends and Challenges in VLSI Circuit Reliability**. IEEE Micro, 2003
  - Wendy Bartlett e Lisa Spainhower. Commercial Fault Tolerance: **A Tale of Two Systems**, IEEE TRANS. ON DEPENDABLE AND SECURE COMPUTING, Jan-Mar 2004.
  - K Reick, PN Sanda, S Swaney, JW Kellington, Michael Mack, Michael Floyd e D. Henderson .FAULT-TOLERANT DESIGN OF THE IBM POWER6 MICROPROCESSOR. IEEE Micro, 2008, pg. 30 a 38
  - P Traverse, I Lacaze, J Souyris. **Airbus fly-by-wire: A total approach to dependability** - Building the Information Society, 2004 - Springer
- livros
  - SURI, N.; WALTER, C.J.; HUGUE, M.M. **Advances in ultra-dependable distributed systems**. IEEE Computer Society Press. Los Alamitos. 1995.