

## Primeira prova

## Revisão da tentativa 1

[Fechar esta janela](#)

<b>Iniciado em</b>	quinta, 23 abril 2009, 10:32
<b>Completado em</b>	quinta, 23 abril 2009, 11:43
<b>Tempo empregado</b>	1 hora 10 minutos
<b>Notas</b>	23/25
<b>Nota</b>	9.2 de um máximo de 10(92%)

Considerando o conceito de cobertura de falhas, assinale a sentença verdadeira:

Escolher uma resposta.

- ☒ a. Capacidade do sistema realizar detecção, recuperação, mascaramento, etc ..
- ☐ b. A cobertura de falhas é computada invertendo a taxa de defeitos.
- ☐ c. Probabilidade condicional que dada uma falha o sistema apresente defeito.
- ☐ d. A cobertura de falhas está relacionada numericamente ao MTTF.
- ☐ e. Relação entre as falhas falsamente sinalizadas pelo mecanismo de tolerância a falhas e as falhas que realmente ocorreram.

Correto

Notas relativas a este envio: 1/1.

Grottke e Trivedi classificam falhas de software em dois tipos: Bohrbugs e Mandelbugs. Assinale a alternativa correta:

Escolher uma resposta.

- ☐ a. Bohrbugs são falhas que provocam um comportamento de software imprevisível e caótico .
- ☒ b. Bohrbugs são falhas que se manifestam consistentemente sob condições bem definidas, ou seja são reproduzíveis.
- ☐ c. Bohrbugs podem ser detectados por testes dinâmicos e Mandelbugs por revisão do código e testes de mesa.
- ☐ d. Mandelbugs são mais fáceis de serem detectados na fase de desenvolvimento do que Bohrbugs.
- ☐ e. Bohrbugs são falhas de hardware que provocam erros no software e Mandelbugs são falhas de software que

Notas relativas a este envio: 1/1.

Grottke e Trivedi classificam falhas de software em dois tipos: Bohrbugs e Mandelbugs. Assinale a alternativa correta:

Escolher uma resposta.

- ☐ a. Bohrbugs são falhas que provocam um comportamento de software imprevisível e caótico .
- ☒ b. Bohrbugs são falhas que se manifestam consistentemente sob condições bem definidas, ou seja são reproduzíveis.
- ☐ c. Bohrbugs podem ser detectados por testes dinâmicos e Mandelbugs por revisão do código e testes de mesa.
- ☐ d. Mandelbugs são mais fáceis de serem detectados na fase de desenvolvimento do que Bohrbugs.
- ☐ e. Bohrbugs são falhas de hardware que provocam erros no software e Mandelbugs são falhas de software que provocam defeito no hardware.

Correto

Notas relativas a este envio: 1/1.

Indique o código de detecção ou correção de erros adequado a cada situação:

Deteção de erros em meios onde é grande a probabilidade de todos os bits estarem grudados em 0.

Paridade bit-per-byte.

Transferências de grandes quantidades de dados.

checksum

Transferências por barramentos com maior probabilidade de falhas que afetam bits adjacentes.

Paridade entrelaçada

Transferências por barramentos com maior probabilidade de falha simples isolada.

Paridade simples

Correto

Notas relativas a este envio: 1/1.

A definição mais próxima de falhas sólidas (hard faults) conforme artigo do Avizienis é:

Escolher uma resposta.

- ☒ a. Falhas cuja ativação é reproduzível.
- ☐ b. Falhas que provocam defeito apenas no hardware.
- ☐ c. Falhas que ocorrem no hardware mas provocam defeito apenas no software.
- ☐ d. Falhas cuja ativação não é sistematicamente reproduzível.

Notas: 1



Correto

Notas relativas a este envio: 1/1.

A definição mais próxima de falhas sólidas (hard faults) conforme artigo do Avizienis é:

Escolher uma resposta.

- ☒ a. Falhas cuja ativação é reproduzível.
- ☐ b. Falhas que provocam defeito apenas no hardware.
- ☐ c. Falhas que ocorrem no hardware mas provocam defeito apenas no software.
- ☐ d. Falhas cuja ativação não é sistematicamente reproduzível.
- ☐ e. Falhas que ocorrem apenas no hardware.

Correto

Notas relativas a este envio: 1/1.

Duplicação de módulos de hardware e comparação das saídas apresenta como vantagem:

Escolher uma resposta.

- ☐ a. Transparência em relação ao software para a recuperação de falhas
- ☐ b. Facilidade de mascarar falhas.
- ☒ c. Simplicidade conceitual e facilidade de implementação para a detecção de falhas
- ☐ d. Baixo custo de implementação do hardware para detecção de falhas
- ☐ e. Facilidade para a localização de falha .

Correto

Notas relativas a este envio: 1/1.

São atributos de dependabilidade:

Escolher uma resposta.

- ☐ a. integridade, correção, tolerância a falhas e consistência
- ☐ b. confiabilidade, disponibilidade, tolerância a falhas e consistência
- ☐ c. tolerância a falhas, remoção de falhas, facilidade de dar manutenção e integridade
- ☐ d. disponibilidade, previsibilidade, segurança (safety) e durabilidade

Correto

Notas relativas a este envio: 1/1.

São atributos de dependabilidade:

Escolher uma resposta.

- ☐ a. integridade, correção, tolerância a falhas e consistência
- ☐ b. confiabilidade, disponibilidade, tolerância a falhas e consistência
- ☐ c. tolerância a falhas, remoção de falhas, facilidade de dar manutenção e integridade
- ☐ d. disponibilidade, previsibilidade, segurança (safety) e durabilidade
- ☒ e. confiabilidade, facilidade de dar manutenção, disponibilidade e segurança (safety)

Correto

Notas relativas a este envio: 1/1.

De acordo com Tanenbaum, os sistemas operacionais são não confiáveis principalmente pelas seguintes razões:

Escolher uma resposta.

- ☒ a. Apresentam pouco isolamento de falhas e são imensos.
- ☐ b. São desenvolvidos por programadores inexperientes para lidar com a complexidade e tamanho de um sistema operacional moderno.
- ☐ c. São tipicamente de código fechado, proprietário, sem comprometimento dos fabricantes com a qualidade .
- ☐ d. Executam sobre hardware de baixa confiabilidade.
- ☐ e. Precisam apresentar alto desempenho, sendo a qualidade um aspecto secundário.

Correto

Notas relativas a este envio: 1/1.

Selecione a alternativa correta.

Escolher uma resposta.

- ☐ a. Como TMR opera com 3 componentes em paralelo, pode suportar falhas em até dois componentes.
- ☒ b. TMR é usado para missões curtas porque sua confiabilidade fica menor do que a de um sistema simplex após um certo tempo de operação.

Notas: 1



- ☐ e. Precisam apresentar alto desempenho, sendo a qualidade um aspecto secundário.

Correto

Notas relativas a este envio: 1/1.

Selecione a alternativa correta.

Escolher uma resposta.

- ☐ a. Como TMR opera com 3 componentes em paralelo, pode suportar falhas em até dois componentes.
- ☒ b. TMR é usado para missões curtas porque sua confiabilidade fica menor do que a de um sistema simplex após um certo tempo de operação.
- ☐ c. TMR é adequado para mascarar falhas de projeto de hardware.
- ☐ d. Em um sistema NMR, quanto maior o N maior a confiabilidade e o desempenho inicial.
- ☐ e. NMR é usado para aumentar o desempenho em sistemas de alta confiabilidade.

Correto

Notas relativas a este envio: 1/1.

Em relação à redundância passiva é correto afirmar que:

Escolher uma resposta.

- ☐ a. A redundância passiva é inadequada para sistemas críticos de tempo real pois exige grande quantidade de componentes e alto consumo de potência.
- ☐ b. A redundância passiva exige o emprego de uma estratégia de detecção de erros com alta cobertura de detecção.
- ☐ c. A redundância passiva envolve detecção e posterior recuperação.
- ☐ d. A redundância passiva é a técnica preferida para sistemas de transações de alta disponibilidade pois suporta longo tempo de missão.
- ☒ e. Redundância passiva é usada para mascarar falhas.

Correto

Notas relativas a este envio: 1/1.

Assinale a alternativa correta.

Correto

Notas relativas a este envio: 1/1.

3 Associe a definição breve com a medida correspondente.

Notas: 1

Tempo médio gasto para reparar um sistema

MTTR

Chances do sistema estar funcionando em um determinado instante

Disponibilidade

Chances do sistema funcionar sem defeitos durante um determinado período de tempo

Confiabilidade

Tempo médio até o próximo defeito

MTTF

Tempo médio entre um defeito e outro

MTBF

Correto

Notas relativas a este envio: 1/1.

4 Considere a seguinte situação: um motorista com alto teor alcoólico acelerou demais o carro que já tinha vários anos de uso, com isso o motor aqueceu e um fio próximo que já estava quase no fim da vida útil se partiu. Esse fio enviava informações sobre a velocidade real ao computador de bordo e, sem essa informação, o computador continuou mandando comandos para acelerar o carro. Como resultado o carro não venceu uma curva e bateu em um poste. O motorista foi preso por dirigir alcoolizado e teve perda total do veículo. Do ponto de vista do sistema computacional:

Notas: 1

Escolher uma resposta.

- ☐ a. não ter efetuado manutenção preventiva foi a falha, dirigir alcoolizado foi erro de operação e não vencer a curva foi o defeito.
- ☐ b. o fim da vida útil do fio foi a falha, não ter redundância na entrada de dados o erro e bater no poste o defeito.
- ☐ c. dirigir alcoolizado foi a falha, não ter comprado um carro novo o erro e a perda total do veículo o defeito
- ☐ d. o fio partido foi a falha, a perda da informação de velocidade na entrada o erro e continuar o envio de comandos para acelerar o carro o defeito
- ☒ e. sobreaquecimento foi a falha, o fio partido o erro e a perda da informação de velocidade na entrada o defeito.

Errado

Notas relativas a este envio: 0/1. Penalidade de 0.1 neste envio

5 Um código RS(28,24) tem capacidade de:

Notas: 1



**Errado**

Notas relativas a este envio: 0/1. Penalidade de 0.1 neste envio

5

Notas: 1

Um código RS(28,24) tem capacidade de:

Escolher uma resposta.

- ☐ a. corrigir 24 bytes errados a cada bloco de 28 bytes
- ☐ b. detectar 28 erros e corrigir 24
- ☒ c. corrigir 2 bytes com erros ou 4 bytes omitidos
- ☐ d. corrigir 24 erros a cada bloco de 28 bits
- ☐ e. corrigir apenas uma rajada de 8 bits

**Correto**

Notas relativas a este envio: 1/1.

6

Notas: 1

A definição: habilidade para evitar defeitos de serviço que sejam mais frequentes e mais severos do que aceitável, se refere a:

Escolher uma resposta.

- ☒ a. dependabilidade
- ☐ b. confiabilidade
- ☐ c. tolerância a falhas
- ☐ d. segurança (safety)
- ☐ e. disponibilidade

**Correto**

Notas relativas a este envio: 1/1.

7

Notas: 1

Considerando as afirmativas abaixo sobre componentes de hardware, assinale a alternativa correta.

Escolher uma resposta.

- ☐ a. A taxa de defeitos de um componente é sempre crescente.
- ☒ b. Durante sua vida útil, componentes apresentam taxa de defeitos aproximadamente constante.
- ☐ c. A taxa de defeitos de um componente é sempre decrescente.

Correto

Notas relativas a este envio: 1/1.

Sobre as estratégias de rollback e rollforward podemos afirmar que:

Escolher uma resposta.

- ☒ a. Apenas rollback é baseada em checkpoints periódicos do estado do sistema e é uma estratégia genérica, independente da aplicação.
- ☐ b. Apenas roolback substitui o estado incorreto por um novo estado nunca ocorrido durante a execução sem erros do sistema.
- ☐ c. Ambas ocorrem após a detecção de erros e substituem o estado incorreto por novo estado livre de erros nunca ocorrido durante a execução do sistema
- ☐ d. Ambas são independentes da aplicação, mas apenas rollforward substitui o estado incorreto por um estado novo nunca ocorrido durante a execução do sistema.
- ☐ e. Ambas ocorrem após a detecção de erros e são estratégias dependentes das características específicas de cada aplicação.

Correto

Notas relativas a este envio: 1/1.

De acordo com Avizienis rollback é uma técnica de:

Escolher uma resposta.

- ☐ a. Reconfiguração.
- ☐ b. Manutenção corretiva.
- ☐ c. Tratamento de falhas.
- ☒ d. Tratamento de erro.
- ☐ e. Detecção de erros.

Correto

Notas relativas a este envio: 1/1.

Assinale a alternativa correta:

Escolher uma

- ☐ a. Uma falha dormiente permanece no sistema nem nunca se manifestar como falha ativa



resposta.

- ☒ b. Evitar introduzir falhas durante projeto e construção do sistema.
- ☐ c. Fornecer serviço esperado mesmo na presença de falhas
- ☐ d. Corrigir as consequências da ocorrência de defeitos.
- ☐ e. Verificar presença de falhas e removê-las.

Correto

Notas relativas a este envio: 1/1.

4  
Notas: 1

Considerando a curva que relaciona taxa de defeitos ao tempo de uso de componentes de hardware a partir da sua fabricação, responda as questões que seguem.

Fase em que os componentes apresentam alta taxa de defeitos após um certo tempo em uso:

envelhecimento

Fase onde é usual se colocar componentes em situação de stress para que os fracos logo apresentem defeitos e possam ser descartados:

mortalidade infantil

Fase usual de operação de componentes:

vida útil

Correto

Notas relativas a este envio: 1/1.

5  
Notas: 1

Entre as técnicas listadas abaixo, quais são as mais adequadas para prevenção de falhas.

Escolher uma resposta.

- ☐ a. redundância de hardware, de software, de informação e temporal
- ☐ b. avaliação qualitativa e avaliação probabilística
- ☐ c. projeto diversitário e programação n-versões
- ☒ d. seleção apropriada de metodologia de projeto, tecnologia e componentes
- ☐ e. verificação, diagnóstico, correção, manutenção preventiva e corretiva

Correto

Notas relativas a este envio: 1/1.

Fechar esta janela

0 Assinale a alternativa correta.

Notas: 1

Escolher uma resposta.

- ☐ a. A redundância sempre implica no aumento do número de componentes de hardware.
- ☐ b. Redundância temporal serve unicamente para detecção de falhas transitórias.
- ☐ c. Redundância temporal serve unicamente para detecção de falhas permanentes.
- ☒ d. Todas as técnicas de tolerância a falhas envolvem o uso de redundância.
- ☐ e. A redundância sempre implica no aumento da confiabilidade de um sistema.

Correto

Notas relativas a este envio: 1/1.

1 Entre as vantagens da programação n-versões podemos citar:

Notas: 1

Escolher uma resposta.

- ☐ a. Facilidade de provar formalmente o aumento de confiabilidade no uso de réplicas.
- ☒ b. Aumento de confiabilidade para pequeno número de réplicas e facilidade de localização dos erros.
- ☐ c. Simplicidade de sincronização de réplicas e diminuição dos custos de desenvolvimento.
- ☐ d. Facilidade para mascarar erros não correlacionados e aumento da confiabilidade do sistema.
- ☐ e. Baixo custo de desenvolvimento e facilidade na detecção de erros.

Errado

Notas relativas a este envio: 0/1. Penalidade de 1 neste envio

2 Assinale a alternativa correta.

Notas: 1

Escolher uma resposta.

- ☐ a. Como o MTTR é muito menor que o MTTF, ele é considerado desprezível para a disponibilidade de um sistema.
- ☐ b. MTTF e MTBF são medidas estatísticas não relacionadas.
- ☐ c. MTTR mede o tempo máximo de reparo de um sistema computacional.
- ☐ d. MTTF mede o tempo médio entre defeitos de um sistema passível de reparo.
- ☒ e. MTTF é inversamente proporcional a taxa de defeitos.

Correto



7 Considerando as afirmativas abaixo sobre componentes de hardware, assinale a alternativa correta.

Notas: 1

Escolher uma resposta.

- ☐ a. A taxa de defeitos de um componente é sempre crescente.
- ☒ b. Durante sua vida útil, componentes apresentam taxa de defeitos aproximadamente constante.
- ☐ c. A taxa de defeitos de um componente é sempre decrescente.
- ☐ d. A taxa de defeitos de um componente depende da tecnologia e condições de uso e não de sua idade.
- ☐ e. A confiabilidade de um componente aumenta com o uso.

Correto

Notas relativas a este envio: 1/1.

8 Assinale a alternativa correta:

Notas: 1

Escolher uma resposta.

- ☐ a. O código de Hamming só pode ser usado para detecção de erros simples.
- ☒ b. A distância de Hamming está diretamente relacionada com a capacidade de correção e detecção de um código.
- ☐ c. Os códigos de Hamming permitem detecção de qualquer falha múltipla unidirecional.
- ☐ d. A distância de Hamming é um conceito que se aplica apenas a códigos de Hamming.
- ☐ e. O código de Hamming é um código não separável.

Correto

Notas relativas a este envio: 1/1.

9 Assinale a afirmativa mais próxima do conceito de defeito de serviço, também chamado abreviadamente de defeito:

Notas: 1

Escolher uma resposta.

- ☒ a. Um defeito é uma transição do serviço correto para um serviço incorreto no qual o sistema se desvia de sua função.
- ☐ b. Um defeito é a causa física ou algorítmica do erro ou do comportamento evasivo de um sistema.
- ☐ c. Um defeito ocorre quando um componente do sistema sofre uma falha permanente ou temporária.
- ☐ d. Um defeito é caracterizado pela ausência de uma especificação para o sistema
- ☐ e. Um defeito é o resultado de ações não autorizadas por parte do operador ou usuário de um sistema.

Correto

1516.JPG - Paint