Tratamento de falhas de software

Revisão da tentativa 1

Iniciado em	terça, 9 outubro 2012, 10:42
Completado em	terça, 16 outubro 2012, 10:55
Tempo empregado	7 dias
Notas	29.4/30
Nota	**98** de um máximo de 100(**98**%)

Question1
Notas: 1

De acordo com o artigo "Fighting Bugs: Remove, Retry, Replicate, and Rejuvenate" de Michael Grottke e Kishor S. Trivedi, publicado na IEEE Computer, em fevereiro de 2007, qual a definição de defeito de sistema (*system failure*)?

Escolher uma resposta.

	a. defeito de sistema ocorre quando o comportamento do sistema conduz a perdas de vidas ou danos irremediáveis ao ambiente ✗
	b. defeito de sistema ocorre quando o comportamento real do sistema leva a prejuízos

	financeiros ✗
◉	c. defeito de sistema ocorre quando o comportamento real do sistema se desvia do serviço correto ✓
○	d. defeito de sistema ocorre quando o sistema trava ✗
○	e. defeito de sistema ocorre quando o comportamento real do sistema se desvia da sua especificação ✗

Correto

Notas relativas a este envio: 1/1.

Question2

Notas: 1

Em que fase do ciclo vida do software o reparo de bugs é mais oneroso (ou seja, apresenta maior custo)?

Escolher uma resposta.

○	a. fase de descarte ✗
○	b. fase de aquisição ✗
○	c. fase de teste ✗
○	d. fase de desenvolvimento ✗
◉	e. fase operacional ✓

Correto

Notas relativas a este envio: 1/1.

Question3

Notas: 1

De acordo com Grottke e Tivedi, o que pode tornar uma tarefa muito difícil o diagnóstico e o isolamento das falhas que são responsáveis por um defeito observável ?

Escolher uma resposta.

- a. o fato de que alguns defeitos não podem ser reproduzidos ✓
- b. o fato dos testadores não dominarem estratégias de teste dinâmicas ✗
- c. o fato dos testadores não dominarem estratégias de teste estáticas ✗
- d. o desconhecimento da especificação do sistema por parte dos testadores ✗
- e. o fato dos desenvolvedores documentarem mal o sistema ✗

Correto

Notas relativas a este envio: 1/1.

Question4
Notas: 1

O que são Bohrbugs?

Escolher uma resposta.

- a. falhas que provocam defeitos que são difíceis de serem reproduzidos ✗
- b. falhas que se manifestam consistentemente sob condições bem definidas ✓
- c. falhas que os métodos tradicionais de teste não conseguem detectar ✗

d. falhas que de acordo com Niels Bohr afetam a estrutura dos átomos ✗

Correto

Notas relativas a este envio: 1/1.

Question5

Notas: 1

Determine se a sentença a seguir é verdadeira ou falsa:
"Toda a ativação de uma falha de software sempre causa um defeito imediatamente pois todas as falhas de software são fixas no código."

Resposta:

Verdadeiro ✗ Falso ✓

Correto

Notas relativas a este envio: 1/1.

Question6

Notas: 1

Determine se a afirmação a seguir é verdadeira ou falsa:
"Uma falha de software, que foi ativada pela execução da parte do código onde a falha está localizada, produz uma condição interna no sistema diferente da condição correta. Essa condição interna é conhecida como erro."

Resposta:

Verdadeiro ✓ Falso ✗

Correto

Notas relativas a este envio: 1/1.

Question7

Notas: 1

Um erro pode se desenvolver em outros erros e assim sucessivamente até que um defeito finalmente ocorra. Essa cadeia de eventos é chamada de:

propagação de erros .

Correto

Notas relativas a este envio: 1/1.

Question8

Notas: 1

Uma instrução mal codificada na implementação de um algoritmo pode levar a um valor incorreto para uma variável de um programa. O programa pode usar esse valor incorreto para computações posteriores levando a incorreções adicionais. Posteriormente, um desses valores incorretos pode influenciar o comportamento observável do sistema.

Considerando o exemplo, associe a descrição ao termo correspondente:

execução do trecho de programa que contém a instrução mal codificada:	erro
incorreções conduzindo a novas incorreções:	propagação de erro
valor incorreto em uma variável:	falha
incorreção observável no comportamento do sistema:	defeito
instrução mal codificada:	ativação da falha

Parcialmente correta

Notas relativas a este envio: 0.4/1.

Question9

Notas: 1

Os autores apresentam **duas** explicações para o software se comportar de forma diferente em situações aparentemente idênticas. São elas:

Escolha pelo menos uma resposta.

- [ ] a. usuários com comportamento caótico e difícil de identificar ✗
- [ ] b. propagação do erro invertida, ou seja, um erro provocando uma falha ✗
- [ ] c. ocorrência de falhas randômicas de hardware ✗
- [x] d. outros elementos do sistema podem influenciar o comportamento da falha numa aplicação específica ✓
- [x] e. longo retardo entre a ativação da falha e a ocorrência do defeito ✓

Correto

Notas relativas a este envio: 1/1.

Question10
Notas: 1

Vários elementos do sistema de software, como o sistema operacional e outras aplicações, podem influenciar o comportamento de uma falha. Um exemplo citado no artigo é a sincronização inadequada de múltiplas threads que, dependendo da ordem do escalonamento das threads, pode provocar comportamentos diferentes. Michael Grottke and Kishor Trivedi nomeia o conjunto desses elementos como:

Escolher uma resposta.

- ○ a. condições de temporização do erro ✗
- ○ b. condições de indeterminismo computacional ✗

c. ambiente interno ao sistema da aplicação ✓

d. escalonamento multithreaded ✗

e. sincronização tempo-real ✗

Correto

Notas relativas a este envio: 1/1.

Question11

Notas: 1

Complete os espaços vazios com os termos correspondentes, de acordo com Grottke e Tivedi:

Uma falha pode fazer com que o software exiba um comportamento caótico e até não determinístico com respeito a ocorrência ou não de defeitos. Profissionais da área se referem a falhas com essa propriedade como Mandelbugs. Algumas vezes, na literatura, essas falhas também são chamadas de Heisenbugs, referindo-se ao fato de que tais falhas trocam seu comportamento quando são observadas ou isoladas.

Correto

Notas relativas a este envio: 1/1.

Question12

Notas: 1

Segundo Michael Grottke e Kishor S. Trivedi, qual o principal problema que o desenvolvedor ou engenheiro de teste enfrenta com bugs que são chamados de Mandelbugs?

Escolher uma resposta.

a. grande probabilidade de serem detectados durante o teste e com isso forçarem o programador a corrigir o código ✗

b. se transformarem em Bohrbugs ✗

c. grande probabilidade de não serem detectados durante o teste ✓

d. envelhecerem e ficarem obsoletos ✗

Correto

Notas relativas a este envio: 1/1.

Question13

Notas: 1

Michael Grottke and Kishor Trivedi afirmam ser plausível concluir que a maioria das falhas que permanecem não detectadas em trechos de software bem testados são de apenas um determinado tipo. Qual o tipo?

Escolher uma resposta.

a. falhas de interação ✗

b. Mandelbugs ✓

c. falhas de temporização ✗

d. falhas de sincronização ✗

e. Bohrbugs ✗

Correto

Notas relativas a este envio: 1/1.

Question14

Notas: 1

Qual a percentagem de falhas detectadas atribuídas a Mandelbugs após a entrada em operação de um software?

Escolher uma resposta.

- a. 1 a 8% ✗
- b. 30 a 40% ✗
- c. 90 a 100% ✗
- d. 15 a 80% ✓

Correto

Notas relativas a este envio: 1/1.

Question15
Notas: 1

De acordo com Grottke e Trivedi, qual a maneira simples e eficiente de lidar com falhas que aparentemente exibem comportamento não determinístico (Mandelbugs) e que não seria adequada para falhas do tipo Bohrbugs?

Escolher uma resposta.

- a. substituição do software ✗
- b. atualização de código ✗
- c. substituição da equipe de desenvolvedores ✗
- d. retentativa, por exemplo restart ou reboot ✓
- e. reprojeto a partir da mesma especificação ✗

Correto

Notas relativas a este envio: 1/1.

Question16

Notas: 1

De acordo com Grottke e Trivedi, a maneira simples e eficiente de lidar com falhas que exibem comportamento não determinístico pode ser melhorada combinando-a com uma técnica conhecida por:

Escolher uma resposta.

○	a. isolamento de falhas ✗
○	b. armazenamento estável ✗
◉	c. checkpointing ✓
○	d. reboot ✗
○	e. detecção de falhas ✗

Correto

Notas relativas a este envio: 1/1.

Question17

Notas: 1

De acordo com Michael Grottke e Kishor S. Trivedi, falhas de software são erros humanos que se escondem no código. Assim, por exemplo, diferentes instalações do mesmo sistema operacional executando as mesmas aplicações deveriam conter as mesmas falhas.

Resposta:

◉ Verdadeiro ✓ ○ Falso ✗

Correto

Notas relativas a este envio: 1/1.

Question18

Notas: 1

Acadêmicos têm discutido que replicação não se aplica a software com as mesmas vantagens obtidas quando aplicada a hardware. Quando se executam comandos em uma segunda instalação para o mesmo software, um usuário vai encontrar as mesmas falhas que levam ao mesmo defeito encontrado na primeira instalação. Grottke e Trivedi concordam com essa argumentação.

Resposta:

Verdadeiro ✗ Falso ✓

Correto

Notas relativas a este envio: 1/1.

Question19

Notas: 1

Acadêmicos têm discutido que replicação não se aplica a software com as mesmas vantagens obtidas quando aplicada a hardware. Quando se executam comandos em uma segunda instalação para o mesmo software, um usuário vai encontrar as mesmas falhas que levam ao mesmo defeito encontrado na primeira instalação. Grottke e Trivedi afirmam que essa argumentação só é válida se todas as falhas forem Bohrbugs.

Resposta:

Verdadeiro ✓ Falso ✗

Correto

Notas relativas a este envio: 1/1.

Question20

Notas: 1

Os autores afirmam que como a maioria da falhas que não se manifestam consistentemente sob condições bem definidas são de fato Mandelbugs, então a replicação de software pode ser considerada útil.

Correto

Notas relativas a este envio: 1/1.

Question21
Notas: 1

Em que situações reiniciar um programa antes de ocorrer um defeito pode reduzir a ocorrência futura de defeitos?

Escolher uma resposta.

- a. quando a taxa de ocorrência de defeitos se mantém constante em relação ao tempo de execução ✗
- b. nunca, isso é uma piada dos autores ✗
- c. quando a taxa de ocorrência de defeitos diminui com o tempo de execução ✗
- d. quando a taxa de ocorrência de defeitos aumenta com o tempo de execução ✓

Correto

Notas relativas a este envio: 1/1.

Question22
Notas: 1

Sistemas de software rodando continuamente durante um longo período de tempo tendem a mostrar um desempenho degradado e uma taxa de defeitos crescente. Esse fenômeno é chamado de:

Escolher uma resposta.

◉	a. envelhecimento de software ✓
○	b. rejuvenescimento de software ✗
○	c. fim da vida útil do software ✗
○	d. inadequação de plataforma de hardware ✗
○	e. obsolescência planejada ✗

Correto

Notas relativas a este envio: 1/1.

Question23
Notas: 1

Sistemas de software rodando continuamente durante um longo período de tempo tendem a mostrar um desempenho degradado e uma taxa de defeitos crescente. Técnicas preventivas contra esse fenômeno são chamadas de:

Escolher uma resposta.

◉	a. rejuvenescimento de software ✓
○	b. replicação de software ✗
○	c. substituição de software ✗
○	d. obsolescência planejada ✗
○	e. envelhecimento de software ✗

Correto

Notas relativas a este envio: 1/1.

Question24
Notas: 1

Porque a taxa de ocorrência de defeitos de um programa aumenta com o tempo sem que o código sofra modificações? Grottke e Trivedi citam duas soluções possíveis a esse quebra-cabeça. Qual a **primeira** solução citada no artigo?

Escolher uma resposta.

◉	a. Bugs podem provocar erros que se acumulam com o tempo (como erros e arredondamento em operações aritméticas). ✓
○	b. O aquecimento provocado por longa operação contínua faz com que bits da memória que contém o código troquem aleatoriamente gerando alterações no programa sendo executado. ✗
○	c. A atenção dos operadores do sistema é influenciada pelo tempo total que o sistema opera continuamente fazendo com que a taxa de falhas de interação aumente sensivelmente. ✗
○	d. O tempo total que o sistema opera continuamente pode influenciar a taxa de ativação de bugs relacionados a envelhecimento. ✗

Correto

Notas relativas a este envio: 1/1.

Question25
Notas: 1

Porque a taxa de ocorrência de defeitos de um programa aumenta com o tempo sem que o código sofra modificações? Grottke e Trivedi citam duas soluções possíveis a esse quebra-cabeça, qual a **segunda** solução citada no artigo?

Escolher uma resposta.

○	a. A atenção dos operadores do sistema é influenciada pelo tempo total que o sistema opera continuamente fazendo com que a taxa de falhas de interação aumente sensivelmente. ✗
◉	b. O tempo total que o sistema opera continuamente pode influenciar a taxa de ativação de bugs relacionados a envelhecimento. ✓
○	c. O acúmulo de atualizações ao longo da vida útil de um software pode aumentar a taxa de bugs em uma dada instalação. ✗
○	d. O aquecimento provocado por longa operação contínua faz com que bits da memória que contém o código troquem aleatoriamente gerando alterações no programa sendo executado. ✗
○	e. Bugs podem provocar erros que se acumulam com o tempo (como erros e arredondamento em operações aritméticas). ✗

Correto

Notas relativas a este envio: 1/1.

Question26

Notas: 1

Bugs relacionados a envelhecimento são Mandelbugs.

Correto

Notas relativas a este envio: 1/1.

Question27

Notas: 1

Rejuvenecimento pode limpar condições de erro internas em um sistema, mas tem como consequência:

Escolher uma resposta.

○	a. necessitar de um conhecimento completo das falhas internas e suas consequências ✗
○	b. maior esforço no desenvolvimento do projeto de software ✗
◉	c. maior custo ✓
○	d. necessidade de monitoramento online ✗
○	e. necessidade de reproduzir e isolar bugs ✗

Correto

Notas relativas a este envio: 1/1.

Question28

Notas: 1

Devido ao custo associado, rejuvenescimento requer otimização do momento de atuação (*optimal timing*). Gottke e Trivedi sugerem duas abordagens para essa otimização. Associe o conceito ao termo:

usa modelos analíticos para capturar a degradação do sistema e necessidade de rejuvenescimento	abordagem baseada em modelos
monitora atributos do sistema que possam mostrar sinais de envelhecimento	abordagem baseada em medidas

Correto

Notas relativas a este envio: 1/1.

Question29

Notas: 1

Devido ao custo associado, rejuvenescimento requer otimização do momento de atuação (*optimal timing*). Gottke e Trivedi sugerem duas abordagens para essa otimização e ilustram com exemplos. Associe o exemplo ao termo:

Considerando uma dada política que determina que um servidor em espera após x horas sem rejuvenescimento deve ser rejuvenecido, os operadores podem usar o modelo para calcular o intervalo ótimo x.	abordagem baseada em modelos
O aumento da quantidade de memória utilizada pode sugerir a existência de falhas na memória que eventualmente podem conduzir a colapso do sistema.	abordagem baseada em medidas

Correto

Notas relativas a este envio: 1/1.

Question30

Notas: 1

Considere as ideias reforçadas na conclusão do artigo de Michael Grottke e Kishor S. Trivedi. Para as sentenças abaixo, responda verdadeiro ou falso de acordo com as afirmações dos autores.

Os autores afirmam que:

Reproduzir e isolar um bug relacionado a envelhecimento é tão simples e fácil como reproduzir e isolar qualquer outro Mandelbug.	Falso
Monitorar por sinais de envelhecimento de software pode ajudar a detectar outras falhas de software que escaparam das avaliações nas fases de desenvolvimento e teste.	Verdadeiro
Rejuvenecimento de software na presença de falhas de envelhecimento só é adequado se os desenvolvedores entendem as falhas e conhecem sua localizão no código.	Falso

Correto

Notas relativas a este envio: 1/1.

INF01209 - Fundamentos de Tolerância a Falhas

Detecção e recuperação em processadores multicore

Revisão da tentativa 1

Terminar revisão

Iniciado em	quinta, 25 outubro 2012, 10:35
Completado em	quinta, 25 outubro 2012, 12:05
Tempo empregado	1 hora 29 minutos

Notas	27.67/28
Nota	**98.81** de um máximo de 100(**99**%)

Question1

Notas: 1

No artigo:

D. Gizopoulos, M. Psarakis, S. V. Adve, P. Ramachandran, S. K. S. Hari, D. Sorin, A. Meixner, A. Biswas, e X. Vera, "Architectures for online error detection and recovery in multicore processors", in Design, Automation Test in Europe Conference Exhibition (DATE), 2011, 2011, p. 1 -6.
a motivação dos autores está relacionada ao fato de que "o enorme investimento no projeto e na produção de processadores multicore pode ser posta em risco por causa das emergentes tecnologias de fabricação altamente miniaturizadas mas não confiáveis". Essas tecnologias podem impor barreiras significativas para a operação confiável ao longo da vida de microprocessadores multicore.

Segundo os autores, microprocessadores fabricados com essas tecnologias serão mais vulneráveis a:

Escolher uma resposta.

a. cortes no orçamento que prejudicam a verificação exaustiva dos chips após a produção; defeitos no processo de fabricação que aceleram o envelhecimento e desgaste que podem produzir erros permanentes; e sobreaquecimento, devido a enorme quantidade de componentes miniaturizados, que reduz o tempo de vida útil. ✗

b. cortes no orçamento que prejudicam a verificação exaustiva dos chips após a produção; defeitos de fabricação latentes, assim como fenômenos de envelhecimento e desgaste que produzem erros permanentes; e interferência eletromagnética cruzada entre os vários núcleos operando em paralelo. ✗

c. stress mecânico e termodinâmico devido a enorme quantidade de componentes miniaturizados dentro do chip; interferência eletromagnética cruzada entre os vários núcleos operando em paralelo; e distúrbios ambientais que produzem erros transitórios. ✗

d. distúrbios ambientais que produzem erros transitórios; defeitos de fabricação latentes, assim como fenômenos de envelhecimento e desgaste que produzem erros permanentes; e ineficiência na verificação que permite que importantes erros de concepção permaneçam no sistema. ✓

Correto

Notas relativas a este envio: 1/1.

Question2

Notas: 1

O foco do artigo de Gizopoulos e demais autores está relacionado a:

Escolher uma resposta.

a. controle da miniaturização durante o processo de fabricação para evitar a vulnerabilidade a falhas externas e de projeto. ✗

b. estratégias de verificação e teste de arquiteturas multicore para evitar falhas de projeto e concepção dos circuitos. ✗

c. arquiteturas de detecção de erros com alta cobertura de detecção para permitir que o microprocessador multicore tenha todos os núcleos em um estado seguro em caso de falha

ativada. ✗

d. arquiteturas confiáveis para processadores multicore que integram soluções para detecção online de erros, diagnóstico, recuperação e reparo durante a fase de operação. ✓

Correto

Notas relativas a este envio: 1/1.

Question3

Notas: 1

Avanços na fabricação de semicondutores têm sustentado a validade da lei de Moore por várias décadas. Recentemente se chegou a conclusão que a única maneira de manter a taxa de aumento de desempenho é:

Escolher uma resposta.

a. melhorar os processos de fabricação ✗

b. construir processadores com vários núcleos (multicore) e explorar o paralelismo. ✓

c. desenvolver microprocessadores tolerantes a falha ✗

d. aumentar o orçamento e melhorar as técnicas de miniaturização ✗

Correto

Notas relativas a este envio: 1/1.

Question4

Notas: 1

Gizopoulos afirma que existe um grande desafio na área de computação que agora é muito mais importante do que já foi anteriormente e se refere a:

Escolher uma resposta.

- (●) a. dependabilidade ✓
- ( ) b. correção ✗
- ( ) c. segurança ✗
- ( ) d. desempenho ✗
- ( ) e. controle do orçamento ✗

Correto

Notas relativas a este envio: 1/1.

Question5

Notas: 1

As 3 fontes mais importantes de operação não confiável do hardware que podem conduzir a defeitos do sistema, de acordo com Gizopoulos. são:

Escolha pelo menos uma resposta.

- [x] a. a variabilidade do processo que faz com que a operação e componentes idênticos no mesmo chip seja diferente (heterogênea) ✓
- [x] b. sensibilidade a erros transientes dos circuitos submicron atuais muito profundos ✓

☐	c. esgotamento da tecnologia de silício que não opera de forma determinística em altas velocidades ✗
☐	d. imperfeições na implementação de estratégias de tolerância a falhas nos circuitos eletrônicos ✗
☑	e. envelhecimento acelerado e/ou desgaste de dispositivos, devido às suas condições de operação extremas ✓

Correto

Notas relativas a este envio: 1/1.

Question6

Notas: 1

Segundo Gizopoulos, além dos problemas causados por erros de hardware que podem afetar gravemente o funcionamento correto de microprocessadores multicore, há outra grande ameaça à operação confiável de dispositivos de hardware. Essa ameça vem piorando continuamente. Qual é essa ameaça?

Escolher uma resposta.

○	a. carência de pessoal compentente ✗
○	b. miniaturização dos componentes ✗
○	c. cortes de orçamento ✗
◉	d. erros e bugs de projeto ✓
○	e. obsolescência acelerada ✗

Correto

Notas relativas a este envio: 1/1.

Question7

Notas: 1

Segundo Gizopoulos, erros de projeto são devidos principalmente a dois fatores:

Escolher uma resposta.

○	a. ausência de estratégias para verificação antes da produção e validação pós-produção ✗
◉	b. grande complexidade e pressão para diminuir o tempo até a comercialização ✓
○	c. falta de domínio dos recursos tecnológicos e indiferença do mercado quanto à qualidade dos dispositivos eletrônicos ✗
○	d. limitação de orçamento e tempo reduzido até a comercialização dos componentes ✗

Correto

Notas relativas a este envio: 1/1.

Question8

Notas: 1

Arquiteturas de processadores multicore incorporam vários núcleos de CPU, memórias (caches, registradores), a lógica de controle de memória e a lógica de interconexão. Memórias ocupam uma grande parte da área do processador, mas podem ser protegidas com sucesso usando técnicas bem conhecidas de redundância como por exemplo:

Escolher uma resposta.

○	a. bit de paridade ✗
○	b. memória estepe ✗
○	c. redundância modular tripla (TMR) ✗
○	d. dupliação e comparação ✗
◉	e. códigos de correção de erros (ECC) ✓

Correto

Notas relativas a este envio: 1/1.

Question9

Notas: 1

Uma vez que a memória é considerada suficientemente protegida, a principal função da detecção de erros é a de proteger o restante do processador: os núcleos, a lógica de controle das memórias e a lógica de interligação.

Várias abordagens para detecção online de erros foram recentemente propostas. Segundo os autores, estas abordagens podem ser classificados em quatro categorias principais.

Assinale a categoria que **não** faz parte das categorias mencionadas pelos autores:

Escolher uma resposta.

a. abordagens de detecção de anomalias. ✗

b. aplicação de auto-teste periódico (BIST) durante a operação usando mecanismos de teste embutidos (built-in). ✗

c. abordagens dinâmicas de verificação. ✗

d. injeção dinâmica de falhas para ativar os mecanismos de detecção de erros. ✓

e. execução redundante que explora a replicação inerente de núcleos e threads do processador. ✗

Correto

Notas relativas a este envio: 1/1.

Question10

Notas: 1

Numa abordagem de execução redundante duas threads (linhas de execução) independentes executam cópias do mesmo programa e os resultados são comparados. Segundo os autores, as duas formas dominantes de execução redundante em microprocessadores são:

Escolher uma resposta.

a. lockstep relaxado e sem lockstep ✗

b. configuração lockstep e multithreading redundante (RMT) ✓

c. simultaneous multithreading (SMT) e multicore (chip multiprocessor) ✗

d. DMR e TMR ✗

e. multithreading redundante (RMT) e TMR ✗

Correto

Notas relativas a este envio: 1/1.

Question11

Notas: 1

A técnica em que núcleos idênticos operam fortemente acoplados "ciclo a ciclo" de clock ou "instrução a instrução" é chamada de:

Escolher uma resposta.

a. CRT ✗

b. lockstep ✓

c. compartihamento de recursos comuns ✗

d. reconfiguração-para-reparo ✗

e. RMT ✗

Correto

Notas relativas a este envio: 1/1.

Question12

Notas: 1

Vários exemplos de detecção de erros online são mostrados no artigo de Gizopoulos. Em um artigo de 2007, alguns autores propuseram configurações DMR e TMR para CMPs (*chip multiprocessor*) que fornecem detecção de erros e recuperação de erros através de confinamento de falhas e isolamento de componentes. Qual o primeiro autor do artigo?

Escolher uma resposta.

- a. Racunas ✗
- b. Aggarwal ✓
- c. Gizopoulos ✗
- d. LaFrieda ✗
- e. Mukherjee ✗

Correto

Notas relativas a este envio: 1/1.

Question13

Notas: 1

Alguns autores propuseram, em um artigo de 2007, configurações DMR e TMR para CMPs que fornecem detecção de erros e recuperação de erros através de confinamento de falhas e isolamento de componentes. A técnica proposta necessita de uma pequena quantidade de área adicional para apoiar o mecanismo de reconfiguração. De quanto aproximadamente é essa área adicional?

Escolher uma resposta.

○	a. aproximadamente 10% em um processador comercial ✗
◉	b. menos de 1% em um processador comercial ✓
○	c. proporcional ao número de núcleos disponíveis no processador ✗
○	d. aproximadamente 5% em um processador comercial ✗

Correto

Notas relativas a este envio: 1/1.

Question14

Notas: 1

Considere as técnicas de detecção online de erros propostas por Mukherjee (CRT), por Gomaa (CRTR) e por Smolens (Reunion). Associe a descrição ao nome da técnica ou técnicas que a emprega(m):

Uma thread mestre em um núcleo é verificada por uma thread escrava em outro núcleo encaminhando seus resultados através de um barramento dedicado.	CRT
Opera com deteção de falhas transientes.	CRTR
Relaxa a replicação de entradas e reduz a largura da banda de comparação comprimindo resultados.	Reunion

Parcialmente correta

Notas relativas a este envio: 0.67/1.

Question15

Notas: 1

Uma alternativa à redundância de hardware é a redundância baseada em software. Segundo os autores, essa alternativa oferece como vantagem:

Escolher uma resposta.

○	a. maior confiabilidade ✗
○	b. maior portabilidade ✗
◉	c. menor custo ✓
○	d. facilidade de aplicar testes ✗
○	e. prova formal de correção ✗

Correto

Notas relativas a este envio: 1/1.

Question16

Notas: 1

Os autores citam dois sistemas que aplicam redundância baseada em software: EDDI e SWIFT. Assinale com X as características que se aplicam aos dois sistemas segundo o artigo.

Assumem que as memórias são protegidas por ECC e por essa razão ficam de fora da esfera de replicação.	-
Todas as instruções são duplicadas e um mecanismo é introduzido para verificar o resultado.	X

São abordagens single-thread mas que servem para processadores com um ou mais núcleos.	X
São abordagens que servem apenas para processadores com apenas um núcleo.	-

Correto

Notas relativas a este envio: 1/1.

Question17

Notas: 1

Outra categoria de abordagens para detecção de erros aproveita o uso de mecanismos de auto-teste embutidos no chip (BIST), tanto em software ou hardware. Este mecanismos são tradicionalmente utilizados para testes de fabricação, mas nessa abordagem eles são ativados durante a fase de operação para detecção de erros.

Abordagens para detecção de erros online baseadas em BIST executam detecção de erro não concorrente. O que significa detecção de erro não concorrente neste contexto?

Escolher uma resposta.

○	a. As sessões de auto-teste são executadas apenas durante o período de inicialização do sistema operacional. ✗
○	b. As sessões de auto-teste são executadas apenas quando disparadas por uma aplicação no nível do usuário. ✗
◉	c. As sessões de auto-teste são executadas periodicamente ou durante intervalos de tempo ociosos. ✓

d. As sessões de auto-teste são executadas apenas durante a fase de mortalidade infantil. ✗

Correto

Notas relativas a este envio: 1/1.

Question18

Notas: 1

Auto-teste baseado em software (SBST) vem mostrando aceitação crescente para teste de microprocessadores nos últimos anos e, atualmente, forma uma parte integrante dos testes durante o processo de fabricação. A idéia-chave do SBST é:

Escolher uma resposta.

a. evitar o uso acidental do hardware embutido que forma o BIST por parte dos programadores de aplicativos. ✗

b. permitir o uso concorrente dos mecanismos de hardware que formam o BIST. ✗

c. aumentar a cobertura das técnicas de detecção de erros providas pelo BIST. ✗

d. explorar recursos programáveis internos ao chip para executar programas normais que testam o processador. ✓

Correto

Notas relativas a este envio: 1/1.

Question19

Notas: 1

Considere as afirmações dos autores a respeito de auto-teste baseado (SBST) em software e assinale Verdadeiro ou Falso:

Com SBST, padrões de testes funcionais são gerados e aplicados pelo processador utilizando o seu conjunto de instruções nativas.	Verdadeiro
SBST virtualmente elimina a necessidade de hardware de teste específico adicional.	Verdadeiro
No SBST o teste é aplicado reduzindo a frequência de funcionamento efetiva do processador.	Falso
A aplicação de testes de software implica uma sobrecarga do sistema uma vez que o tempo do teste periódico pode consumir entre 5% e 25% do tempo do sistema.	Verdadeiro
Devido a problemas de sincronização, não é possível aplicar SBST a processadores multithread.	Falso

Correto

Notas relativas a este envio: 1/1.

Question20

Notas: 1

Outra categoria de abordagens para detecção de erro que, assim como auto teste, não usa execução redundante é a verificação dinâmica. Essas abordagens de verificação dinâmica funcionam em tempo de execução e usam verificadores de hardware dedicados. Para que servem esses verificadores?

Escolher uma resposta.

a. para verificar a integridade de votadores, comparadores e detectores de erros implementados em hardware. ✗

b. para comparar o resultado de duas threads simultâneas. ✗

c. para detectar anomalias semânticas no software em execução. ✗

d. para verificar a validade de invariantes específicos assumidos verdadeiros durante operação normal sem erros. ✓

e. para detectar anomalias nos dados através de bits de paridade. ✗

Correto

Notas relativas a este envio: 1/1.

Question21

Notas: 1

A abordagem de verificação dinâmica usada para detecção online de erros tem um ponto chave. Segundo os autores, esse ponto chave consiste em:

Escolher uma resposta.

a. definir a complexidade e a área ocupada pelo verificador ✗

b. definir um conjunto abrangente de padrões de teste ✗

c. determinar a cobertura de erros da técnica de detecção empregada ✗

d. definir um conjunto compreensivo de invariantes ✓

Correto

Notas relativas a este envio: 1/1.

Question22

Notas: 1

Gizopoulos, Psarakis e Vera apresentam dois exemplos de propostas de aplicação de verificação dinâmica: DIVA e Argus. Considerando esses dois sistemas no contexto de verificação dinâmica para detecção online de erros, assinale verdadeiro ou falso:

Infelizmente DIVA impõe um custo muito alto em termos de desperdício de área para um núcleo superescalar complexo.	Falso
Para processadores simples usualmente usados em arquiteturas multicore, a complexidade do verificador é comparável ao do núcleo, o que aumenta significativamente o custo.	Verdadeiro
Argus usa um número grande de invariantes, tipicamente mais que 17, para alcançar uma cobertura de falhas da ordem de 98%.	Falso
DIVA usa um núcleo verificador simples para detectar erros em um núcleo superescalar especulativo.	Verdadeiro

Correto

Notas relativas a este envio: 1/1.

Question23

Notas: 1

A quarta categoria de detectores de erros online é formada por abordagens de detecção de anomalias. De que forma essa abordagem detecta erros?

Escolher uma resposta.

- a. monitorando o hardware procurando sinais elétricos instáveis e variação na frequência de clock ✗
- b. monitorando o sistema quanto a variações bruscas de temperatura que provocam anomalias nos valores transmitidos entre as unidades funcionais internas ✗
- c. monitorando o software procurando por comportamentos anômalos, também chamados de sintomas ✓
- d. monitorando os barramentos de hardware procurando por indicação de erro de paridade ✗

Correto

Notas relativas a este envio: 1/1.

Question24

Notas: 1

As abordagens de detecção de anomalias pode ser classificados em três categorias de acordo com o nível dos sintomas que elas detectam. As 3 categorias de detecção de anomalias são:

Escolher uma resposta.

- a. as que detectam anomalias no valor dos dados; as que detectam anomalias de comportamento da microarquitetura; e as que detectam anomalias de comportamento do software. ✓
- b. as que detectam anomalias na memória cache interna; as que detectam dados duplicados ou ausentes; e as que detectam anomalias de comportamento dos componentes do sistema operacional

como o escalonador de processos e o gerente de memória virtual. ✗

c. as que detectam anomalias no endereçamento dos dados na memória; as que detectam anomalias no tratamento de exceções; e as que detectam anomalias de comportamento do kernel do sistema operacional. ✗

Correto

Notas relativas a este envio: 1/1.

Question25

Notas: 1

Abordagens eficientes para tomada de pontos de verificação (checkpointing) e para recuperação têm sido propostas para arquiteturas multicore. Essas abordagens são classificadas em 3 categorias:

Escolher uma resposta.

a. periodicidade dos checkpoints, localização relativa dos checkpoints; e esfera da recuperação ✗

b. periodicidade dos checkpoints, localização relativa dos checkpoints; e velocidade da recuperação ✗

c. esfera de recuperação; localização relativa dos checkpoints; e separação entre dados e checkpoints ✓

d. recuperação por avanço; recuperação por retorno; e mascaramento de falhas ✗

Correto

Notas relativas a este envio: 1/1.

Question26

Notas: 1

Os autores citam duas propostas que implementam recuperação por retorno em processadores multicore: SafetyNet e Revive. Associe a característica ao sistema:

pode tolerar latência de detecção de falhas de até 1 ms	SafetyNet
combina o ponto de verificação local e o registro incremental de dados e armazena as atualizações em buffers especiais	SafetyNet
pode tolerar latência de detecção de falhas de até 100 ms	Revive
usa pontos de verificação globais, libera linhas sujas (alteradas) de cache para a memória principal e usa um controlador especial para registrar as atualizações de memória na memória	Revive

Correto

Notas relativas a este envio: 1/1.

Question27

Notas: 1

Técnicas de reparo tipicamente aplicam redundância (espacial ou temporal) para desativar e isolar o componente defeituoso. Arquiteturas de processadores superescalares complexas possuem redundância inerente com a finalidade original de fornecer maior desempenho e execução especulativa. Assim, os componentes redundantes e não essenciais podem ser desativados em caso de falha permitindo degradação suave do desempenho (graceful degradation). Essa solução entretanto não é geralmente útil para arquiteturas muticore. Qual a razão?

Escolher uma resposta.

○	a. arquiteturas multicore visam alto desempenho e não é permitido degradar desempenho para garantir confiabilidade ✗
○	b. multiprocessadores multicore são usados em aplicações convencionais que não necessitam confiabilidade ✗
○	c. multiprocessadores multicore são construídos de forma a não apresentar defeito em seus componentes internos e, portanto, técnicas de isolamento e reparo são desnecessárias ✗
◉	d. os núcleos de uma arquitetura multicore são geralmente muito simples e não apresentam grau suficiente de redundância inerente necessário para desativar componentes e continuar operando ✓

Correto

Notas relativas a este envio: 1/1.

Question28

Notas: 1

Várias abordagens foram propostas para reparo em em sistemas multicore. Associe a breve descrição à proposta:

O software é modificado de modo a preservar a sua funcionalidade mas a não utilizar os componentes defeituosos.	Detouring
Permite a canibalização dos núcleos em peças de reposição, onde essas peças podem ser estágios de pipeline.	Core Cannibalization
Arquitetura concebida como uma rede reconfigurável de estágios de pipeline, em vez de núcleos isolados. Os estágios de pipeline atuam como elementos de processamento e são compartilhados entre	StageNet

os núcleos fornecendo redundância de grão fino.

Correto

Notas relativas a este envio: 1/1.

Terminar revisão

INF01209 - Fundamentos de Tolerância a Falhas

Segurança funcional crítica

Revisão da tentativa 1

Terminar revisão

Iniciado em	quinta, 8 novembro 2012, 10:42
Completado em	quinta, 8 novembro 2012, 11:22
Tempo empregado	40 minutos 2 segundos

Notas	23.4/25
Nota	**93.6** de um máximo de 100(**94**%)

Question1

Notas: 1

William Dunn, no artigo Designing Safety-Critical Computer Systems, publicado na Computer em 2003, cita várias exemplos de aplicações de segurança crítica. Assinale com X aplicações de segurança crítica citadas pelo autor.

processamento químico e de petróleo	X
controles de vôo (fly-by-wire) de aeronaves	X
base de dados de hóspedes em um hotel	-
sistemas de suporte a vida em hospitais	X
editores de texto	-
controle de mercadorias em um supermercado	-
sistemas financeiros online como bolsa de ações e mercadorias	-

Correto

Notas relativas a este envio: 1/1.

Question2

Notas: 1

William Dunn cita alguns exemplos de aplicações de segurança crítica que vão afetar a vida de todos. Assinale com X os exemplos de segurança crítica citadas pelo autor nesta categoria.

sistemas de controle automotivos embarcados	-
controle automatizado de tráfego aéreo e de superfície	X
próteses eletrônicas	X
pagamentos através de telefones celulares e outros dispositivos móveis	-
monitoramento de frequência de estudantes em uma rede pública de ensino	-

Parcialmente correta

Notas relativas a este envio: 0.8/1.

Question3

Notas: 1

Segundo William R. Dunn, qual é a principal preocupação relacionada ao uso de sistemas baseados em computadores?

Escolher uma resposta.

◉	A. Eles podem eventualmente falhar e causar grandes danos, como já foi observado no passado. ✓
○	B. A sua ubiquidade. ✗
○	C. A vida útil do sistema, que por força do constante avanço da tecnologia, tente a encurtar muito rapidamente. ✗
○	D. A ineficiência destes sistemas, se comparados a sistemas eletro-mecânicos tradicionais. ✗
○	E. O custo inerente à manutenção destes sistemas. ✗

Correto

Notas relativas a este envio: 1/1.

Question4

Notas: 1

Dunn cita um grave acidente que ocorreu devido ao uso do Therac25. O que era o Therac25?

Escolher uma resposta.

○	A. Era um sistema de gestão hospitalar muito popular nos anos 80, principalmente nos Estados Unidos. ✗
○	B. Era um processador tolerante a falhas especialmente projetado para sistemas terapêuticos, que ajudou na evolução da medicina computacional. ✗

◉	C. Era um sistema de computador terapêutico destinado a curar pacientes, mas que inadvertidamente matou e mutilou muitas pessoas antes de ser forçado a sair do mercado. ✓
○	D. Era um sistema de computador terapêutico destinado a curar pacientes, mas devido à falta de evidências de sua eficácia, foi forçado a sair do mercado. ✗

Correto

Notas relativas a este envio: 1/1.

Question5

Notas: 1

Na prática, muitos conceitos e arquiteturas vistas como seguras por seus desenvolvedores falharam, colocando pessoas, propriedades ou o ambiente em risco. Segundo William Dunn, isto aconteceu principalmente porque seus autores ou usuários... (marque as 3 razões principais):

Escolha pelo menos uma resposta.

☐	A. não estavam dispostos a pagar o custo adicional relacionado aos conceitos e estruturas de segurança ✗
☑	B. esqueceram de considerar o sistema principal no qual o conceito de segurança a ser aplicado era para ser incorporado. ✓
☑	C. tinham uma compreensão incompleta do que faz um sistema ser "seguro". ✓
☐	D. não se preocuparam em monitorar as possíveis falhas. ✗
☑	E. ignoraram pontos únicos de falha, que fizeram o conceito de segurança irreal quando posto em prática. ✓

F. não sabiam implementar as possíveis soluções seguras adequadas às suas necessidades. ✗

Correto

Notas relativas a este envio: 1/1.

Question6

Notas: 1

Segundo o William Dunn, rever as definições e conceitos fundamentais de segurança de sistemas já implementados nos fornece uma estrutura para tratar os problemas relacionados à área. O que pode auxiliar, segundo o autor, a verificar se o projeto destes sistemas será seguro?

Escolher uma resposta.

A. Testar continuadamente por um longo período os sistemas, antes de coloca-los em funcionamento. ✗

B. Explorar o projeto sistemático de sistemas de computadores seguros. ✓

C. Utilizar técnicas de mapeamento dinâmico de pontos críticos no projeto quando este está em uso. ✗

D. Controlar sua temperatura em períodos longos de funcionamento. ✗

Correto

Notas relativas a este envio: 1/1.

Question7

Notas: 1

Localize-se no item "definindo segurança". Qual é o significado do termo *mishap* segundo o Departamento de Defesa dos EUA?

Escolher uma resposta.

○	A. Gravidade de um acidente determinado em valores financeiros. ✗
○	B. Consequência de um acidente ou infortúnio imprevisto. ✗
○	C. Azar, infelicidade, contrariedade, contratempo, sem maiores consequências ✗
○	D. Evento resultante diretamente de uma falha humana, que resulta em morte, lesão, doença ocupacional, danos e perda de equipamento ou bens, ou danos ao meio ambiente. ✗
◉	E. Evento imprevisto ou uma série de eventos que resultam em morte, lesão, doença ocupacional, danos e perda de equipamentos ou bens, ou danos ao meio ambiente. ✓

Correto

Notas relativas a este envio: 1/1.

Question8

Notas: 1

Qual é o significado de *mishap risk* (risco de acidente) segundo Willian Dunn?

Escolher uma resposta.

○	A. É a avaliação do risco estatístico de perda financeira relacionado a ocorrência de um acidente. ✗
○	B. É a avaliação do impacto de um acidente em termos de duas preocupações principais: danos a

	vidas humanas e danos financeiros. ✗
○	C. É uma avaliação da probabilidade de ocorrência de um acidente desconsiderando a sua severidade. ✗
◉	D. É a avaliação do impacto de um acidente em termos de duas preocupações principais: a sua gravidade potencial e a probabilidade de sua ocorrência. ✓

Correto

Notas relativas a este envio: 1/1.

Question9

Notas: 1

Considerando as ideias e conceitos expressas por William Dunn, responda se as sentenças são verdadeiras ou falsas.

Na criação de um sistema seguro, minimizar os custos de redução de riscos de acidentes (mishap risks) nos obriga a um comprometimento do sistema, na medida em que gastamos recursos. Mas pode-se fazer isto somente até um nível considerado aceitável em geral.	Verdadeiro
Sistemas tais como automóveis, aviões e as usinas nucleares não são absolutamente (ou seja, 100%) seguros.	Verdadeiro
Dada a atual tecnologia, é possível eliminar os riscos de acidentes em sistemas de segurança críticos.	Falso
Em algumas aplicações, a redução de riscos de acidentes domina completamente os custos do sistema.	Verdadeiro

Correto

Notas relativas a este envio: 1/1.

Question10

Notas: 1

Localize-se no item "riscos aceitáveis de acidentes". O que é considerado um risco aceitável para um determinado tipo de acidente por parte do grande público, se acordo com Willian Dunn?

Escolher uma resposta.

○	A. Só é considerado aceitável um risco zero de acidentes. ✗
○	B. Enquanto há um risco, este nunca será considerado aceitável. ✗
○	C. O grande público não se preocupa com aspectos técnicos e mostra disposição de aceitar qualquer risco. ✗
◉	D. Basicamente, enquanto os acidentes ocorrerem muito infrequentemente seu risco é considerado aceitável. ✓
○	E. Risco aceitável para um acidente é determinado pela ausência de acidentes daquele tipo até o momento. ✗

Correto

Notas relativas a este envio: 1/1.

Question11

Notas: 1

Segundo as estatísticas, qual é a taxa aceitável de risco de acidentes comuns?

Escolher uma resposta.

○	10^2 a 10^10 acidentes por hora. ✗
○	10^-2 a 10^-10 acidentes por dia. ✗
◉	10^-2 a 10^-10 acidentes por hora. ✓
○	Não existem dados considerados confiáveis para determinar tal taxa de acidentes. ✗

Correto

Notas relativas a este envio: 1/1.

Question12

Notas: 1

Dunn afirma que apesar dos resultados trágicos dos acidentes de trânsito, a maioria das pessoas se sente segura dirigindo um carro. Qual seria a razão para essa sensação de segurança?

Escolher uma resposta.

○	A. a desinformação da maioria das pessoas a respeito da frequência dos acidentes de carro ✗
○	B. a falta de formação tecnológica das pessoas ✗
◉	C. a raridade da ocorrência de acidentes ✓
○	D. ao fato do custo de um acidente de carro ser relativamente baixo comparado com um acidente na aviação ✗

Correto

Notas relativas a este envio: 1/1.

Question13

Notas: 1

Considerando o conceito de risco aceitável, um projeto de um computador para ser usado na área de segurança crítica com uma chance de 10% de acidente catastrófico por hora de operação pode ser considerado um sistema seguro?

Escolher uma resposta.

○	A. Não, deve ser no mínimo de 1%. ✗
○	B. Depende do propósito da aplicação. ✗
◉	C. Não, é uma taxa de acidentes altíssima. ✓
○	D. Não é possível usar computadores na área de segurança crítica pois é sabido que computadores apresentam baixa confiabilidade. ✗
○	E. Sim, se está dentro do planejado pelos projetistas. ✗

Correto

Notas relativas a este envio: 1/1.

Question14

Notas: 1

Quem decide o que é um risco aceitável?

Escolher uma resposta.

○	A. os projetistas de sistemas baseados no seu conhecimento técnico e julgamento ético ✗
○	B. a comunidade diretamente afetada através de voto direto ✗
○	C. os consumidores de produtos tecnológicos ✗
◉	D. as associações industriais, sociedades profissionais de segurança e institutos relacionados a segurança que assumem o consenso do público em geral sobre riscos aceitáveis e os transformam em padrões e leis ✓
○	E. a própria empresa que implementa e comercializa a solução segura ✗

Correto

Notas relativas a este envio: 1/1.

Question15

Notas: 1

Mil-STD-882 D e IEC 61508 são:

Escolher uma resposta.

○	A. relatos de acidentes governamentais e industriais repectivamente ✗
○	B. leis internacionais que regulam aspectos de segurança ✗
○	C. textos motivacionais para alertar governos e indústrias acerca dos cuidados com segurança ✗

D. normas de segurança ✓

Correto

Notas relativas a este envio: 1/1.

Question16

Notas: 1

Tipicamente qualquer computador, seja um controlador de vôo de uma aeronave, um robô industrial ou uma máquina de radiação terapêutica, é composto, segundo Dunn, de cinco componentes primários. Relacione os componentes primários de um sistema de computação com sua função.

Humano responsável por monitorar e ativar em tempo real o sistema	Operador
Componente que converte um sinal elétrico de saída do computador para uma ação física correspondente que controla a função de um aplicativo.	Atuador
Entidade física que o sistema monitora e controla, muitas vezes chamada de planta ou processo.	Aplicação
Composto de hardware e software que monitora e controla a aplicação em tempo real.	Computador
Componente que converte uma medida física em um sinal elétrico correspondente para a entrada no computador.	Sensor

Correto

Notas relativas a este envio: 1/1.

Question17

Notas: 1

Dunn cita alguns exemplos para componentes de um sistema de computação. Associe os exemplos aos nomes dos componentes.

acelerômetro	sensor
válvula	atuador
controlador lógico programável	computador
transdutor de pressão	sensor
motor	atuador

Correto

Notas relativas a este envio: 1/1.

Question18

Notas: 1

Dunn cita alguns modelos de computador que monitoram e controlam aplicações em tempo real. Assinale entre os modelos abaixo um exemplo que não forma um sistema de computação.

Escolher uma resposta.

A. Controlador em placa única. ✗

◉	B. Instrumentos de campo. ✗
○	C. Computador de bordo em aviões. ✗
○	D. Conjunto de sensores. ✓
○	E. CLP - Controlador lógico-programável ✗

Errado

Notas relativas a este envio: 0/1.

Question19

Notas: 1

Localize-se no item "análise de hazards" do artigo de Willian Dunn. O que se pode afirmar quanto a sistemas básicos de computadores?

Escolher uma resposta.

○	A. Com a tecnologia atual, sistemas básicos já são suficientemente seguros para qualquer tipo de aplicação. ✗
○	B. É impossível ter um sistema básico que apresente uma taxa de risco de acidentes em um nível aceitável ✗
◉	C. Como sistemas básicos não empregam recursos de segurança, provavelmente irão apresentar um nível muito elevado de risco de acidente. ✓
○	D. Projetos seguros são geralmente muito complexos, e estes elementos básicos que compõe o sistema têm pouca ou nenhuma influência na taxa de risco de acidentes. ✗

Correto

Notas relativas a este envio: 1/1.

Question20

Notas: 1

Quando um sistema de computação básico apresentar um nível inaceitável de risco de acidente, qual a solução apontada por Dunn.

Escolher uma resposta.

○	a. A solução exige encontrar uma nova solução que não necessite o uso de computadores. ✗
○	b. A solução exige adotar uma rede complexa de sistemas básicos. ✗
◉	c. A solução exige modificar a operação, os sensores, os atuadores e o computador para criar um novo sistema que estará dentro do nível aceitável de risco. ✓
○	d. A solução exige modificar a aplicação para que ela não exiba um nível tão alto de risco. ✗

Correto

Notas relativas a este envio: 1/1.

Question21

Notas: 1

Quando um sistema básico exibe um nível inaceitável de risco, o projeto de uma solução inicia com qual questão?

Escolher uma resposta.

◉	A. Como pode este sistema de computação básico apresentar defeito e causar um acidente? ✓
○	B. De que maneira é possível minimizar os danos em caso de acidente por falha no sistema? ✗
○	C. Quais as consequências de um possível acidente causado por este sistema básico? ✗
○	D. Quão custosa será a solução para o problema? ✗

Correto

Notas relativas a este envio: 1/1.

Question22

Notas: 1

O elemento chave que conecta um defeito em um sistema básico de computação a um acidente subsequente é chamado de:

Escolher uma resposta.

○	a. failure ✗
○	b. mishap risk ✗
○	c. mishap ✗
◉	d. hazard ✓
○	e. error ✗

Correto

Notas relativas a este envio: 1/1.

Question23

Notas: 1

De acordo com Willian Dunn, no contexto de segurança crítica, *hazard* é qualquer condição real ou potencial que pode causar:

Escolher uma resposta.

◉	A. lesões, doença ou morte de pessoas; danos ao meio ambiente; danos a ou perdas de sistemas, equipamentos ou propriedade ✓
○	B. erros não detectáveis no equipamento; falhas difíceis de serem localizadas, isoladas e/ou compensadas; alta latência de falha; defeitos de causa comum ✗
○	C. insatisfação dos operadores de um sistema básico de segurança; stress ocupacional; falhas humanas involuntárias provocadas por fadiga do operador ✗
○	D. perdas financeiras; danos a propriedade; perdas de equipamentos e de credibilidade no mercado de prestação de serviços ✗

Correto

Notas relativas a este envio: 1/1.

Question24

Notas: 1

Segundo o autor, são exemplos de *hazards* contidos na aplicação: (escolha 3 exemplos)

Escolha pelo menos uma resposta.

☑	A. esfriamento do núcleo em uma central nuclear ✓
☐	B. bit-flip na memória do sistema básico de computação ✗
☑	C. presença de material tóxico ou gás natural ✓
☑	D. perda de controle de vôo ✓
☐	E. leitura incorreta de informação de temperatura ✗

Correto

Notas relativas a este envio: 1/1.

Question25

Notas: 1

Para finalizar a leitura do item "análise de hazards", enumere a sequência de ações a serem tomadas para um projeto de um sistema seguro.

Análise do operador, sensor, computador e atuador.	2
Com base nas informações coletadas, estabelecimento de uma ligação entre todos os modos possíveis de defeitos e os acidentes.	4
Análise de modos de defeitos de cada componente, para determinar todas as suas fontes de defeitos incluindo defeitos de hardware, problemas de fabricação, falhas de programação, stress ambiental, erros de projeto e erros na manutenção.	3

Início do projeto real, levando em consideração as análises anteriores.	1
Identificação dos hazards na aplicação do sistema.	5

Parcialmente correta

Notas relativas a este envio: 0.6/1.

Terminar revisão

Análise e redução de risco

Revisão da tentativa 1

Iniciado em	segunda, 12 novembro 2012, 13:01
Completado em	domingo, 18 novembro 2012, 23:13
Tempo empregado	6 dias 10 horas
Notas	25.08/26
Nota	**96.47** de um máximo de 100(**96**%)

Question1
Notas: 1

Localize-se no item "um exemplo simples" no artigo: Dunn, W.R. "Designing Safety-critical Computer Systems." Computer 36, no. 11 (2003): 40– 46.

No exemplo simples, assinale ***hazard*** (perigo), ***mishap*** (acidente, sinistro) e **defeito** para os eventos descritos abaixo:

operador sofre queimaduras por ter aberto uma saída de água estando a água sobreaquecida	mishap
sensor de temperatura marcando temperatura abaixo da temperatura real da água	defeito

sobreaquecimento da água	hazard
a explosão do tanque de água causada pelo sobreaquecimento da água além do ponto de ebulição	mishap
a interface de hardware do computador comanda permanentemente "manter aquecimento" para a unidade de aquecimento de água	defeito

Correto

Notas relativas a este envio: 1/1.

Question2

Notas: 1

Considerando que um sistema pode apresentar um alto risco de acidente (*mishap*), Dunn cita 3 formas de diminuir o risco. Assinale as 3 formas:

Escolha pelo menos uma resposta.

☐	a. incorporar dispositivos de segurança internos ✓
☐	b. escolher uma boa equipe de desenvolvedores ✗
☑	c. aumentar a qualidade e a confiabilidade dos componentes ✓
☑	d. usar ferramentas de desenvolvimento certificadas ✗
☑	e. incorporar dispositivos de segurança externos ✓

Parcialmente correta

Notas relativas a este envio: 0.33/1.

Question3

Notas: 1

Melhorar a confiabilidade visa a:

Escolher uma resposta.

- a. reduzir a probabilidade de defeito de componente, o que, por sua vez, reduz a probabilidade de acidente (mishap) ✓
- b. aumentar a vida útil de um componente, o que, por sua vez, aumenta a vida útil do sistema e com isso reduz os custos associados à manutenção ✗
- c. zerar a probabilidade de ocorrência de defeitos ✗
- d. eliminar as fontes que potencialmente causam defeitos de componentes ✗

Correto

Notas relativas a este envio: 1/1.

Question4

Notas: 1

De acordo com Dunn, existe uma abordagem muito usada e eficiente para aumentar a confiabilidade de um sistema. Determine qual seria essa abordagem:

Escolher uma resposta.

- a. aplicação de medidas que aumentem a qualidade do sistema ✗
- b. uso de componentes redundantes de software e hardware ✓
- c. certificação do sistema pela IEC 61508 ✗

d. evitar problemas que resultam de condições ambientais impróprias ✗

e. reprojeto ✗

Correto

Notas relativas a este envio: 1/1.

Question5

Notas: 1

No artigo são mencionadas fontes responsáveis por defeito de componentes que são, nas palavras do autor, mais evasivas, como por exemplo: erros humanos, inadequação de projeto e deficiências nos procedimentos. A norma IEC 61508 inclui essas fontes de defeitos em uma categoria geral descrita como:

Escolher uma resposta.

a. defeitos randômicos ✗

b. defeitos elusivos ✗

c. defeitos maliciosos ✗

d. defeitos sistemáticos ✓

e. defeitos evasivos ✗

Correto

Notas relativas a este envio: 1/1.

Question6

Notas: 1

No artigo são mencionadas fontes de defeito de componentes mais evasivas, como: erros humanos, inadequação de projeto e deficiências nos procedimentos. Para evitá-los ou eliminá-los, a norma IEC 61508 recomenda:

Escolher uma resposta.

- a. abordagens orientadas a qualidade ✓
- b. abordagens baseadas em automação de projeto sem interferência humana ✗
- c. evitar usar componentes de software ✗
- d. abordagens orientadas a redundância ✗
- e. reprojeto do sistema ✗

Correto

Notas relativas a este envio: 1/1.

Question7
Notas: 1

Segundo Willian Dunn, quando são necessários dispositivos internos de segurança?

Escolher uma resposta.

- a. quando o projeto usou componentes de baixa confiabilidade ✗
- b. quando se deseja reduzir os custos além de reduzir os riscos ✗
- c. quando o projeto foi mal especificado e ninguém conhece como ele vai se comportar em operação real ✗

○	d. quando redundância se torna economicamente inviável ✗
◉	e. quando o projeto requer passos adicionais para reduzir os riscos abaixo do nível de risco alcançado pelas medidas de qualidade e confiabilidade ✓

Correto

Notas relativas a este envio: 1/1.

Question8

Notas: 1

Segundo Willian Dunn, os dispositivos internos de segurança, além de reduzir os efeitos de falhas de hardware e software, também fornecem:

Escolher uma resposta.

○	a. uma barreira contra operadores humanos ✗
○	b. uma barreira que evita a ocorrência de falhas de software e hardware ✗
◉	c. uma barreira contra defeitos sistemáticos ✓
○	d. uma solução de baixo custo para evitar acidentes ✗

Correto

Notas relativas a este envio: 1/1.

Question9

Notas: 1

A última linha de defesa contra defeitos que podem resultar em acidentes (*mishaps*) é provida por dispositivos que atuam quando a aplicação experimenta um evento perigoso. Esses dispositivos são conhecidos por:

Escolher uma resposta.

a. dispositivos internos de segurança ✗

b. dispositivos externos de segurança ✓

c. dispositivos especializados em segurança ✗

d. dispositivos de alta confiabilidade ✗

e. dispositivos redundantes ✗

Correto

Notas relativas a este envio: 1/1.

Question10

Notas: 1

Para alcançar efetiva redução de risco de acidentes, os projetistas costumam:

Escolher uma resposta.

a. evitar defeitos sistemáticos ✗

b. usar as 3 formas de redução de risco de forma balanceada e evitando negligenciar alguma parte do sistema ✓

c. enfatizar qualidade e confiabilidade dos componentes de hardware e software ✗

d. enfatizar dispositivos externos de segurança pois são mais baratos e eficientes que os demais recursos de segurança ✗

e. enfatizar dispositivos internos de segurança pois são mais baratos e eficientes que os demais recursos de segurança ✗

Correto

Notas relativas a este envio: 1/1.

Question11

Notas: 1

Considerando o exemplo do aquecedor de água, apresentado por Dunn, associe o recurso usado no exemplo com uma das 3 estratégias de redução de riscos:

1 - melhorar a confiabilidade e confiabilidade dos componentes

2 - incorporar dispositivos internos de segurança

3 - incorporar dispositivos externos de segurança

programa que detecta defeito em vários componentes e então atua sobre uma chave de potência para desligar o equipamento	2
uso de uma chave de limitação de alta temperatura	2
componentes com confiabilidade superior aos usados em equipamentos convencionais	1
cuidados para garantir integridade estrutural do tanque de água	1
válvula de alívio de temperatura e pressão	3

Correto

Notas relativas a este envio: 1/1.

Question12

Notas: 1

A figura 4 do artigo do Dunn mostra dispositivos adicionais de segurança e algumas técnicas usados para redução de risco encontradas em aplicações da vida-real. Associe o nome do recurso à sua forma de atuação:

detecta defeitos em sensores individuais	redundância de informação
detecta defeitos em atuadores realimentando a saída do atuador no computador para verificar se a saída corresponde ao comando enviado	w raparound
inibe ação do atuador (effector) a menos que alguma condição física externa seja satisfeita	intertravamento
verifica a integridade do sistema de entrada e saída do computador	endaround
inibe as saídas do atuador (effector) forçando o sistema para um estado seguro	circuito de parada de emergência
inibe a ação do atuador (effector) se o computador (ou o software) apresentar defeito e parar de enviar pulsos indicando que está em operação	w atchdog timer

Correto

Notas relativas a este envio: 1/1.

Question13

Notas: 1

Dispositivos de segurança adicional implementam técnicas de redução de risco. Uma dessas técnicas consiste em inibir ação do atuador (effector) a menos que alguma condição física externa seja satisfeita. Dunn ilustra como exemplo da aplicação da técnica uma chave na porta de um fogão de microondas que encerra o cozimento quando a porta do microondas é aberta. O exemplo apresentado se refere a técnica de:

Escolher uma resposta.

○	a. detecção de falhas no sensor ✗
○	b. watchdog timer ✗
○	c. parada de emergência ✗
○	d. wraparound ✗
◉	e. intertravamento ✓

Correto

Notas relativas a este envio: 1/1.

Question14

Notas: 1

Considere os conceitos de sistemas *fail-safe* e sistemas *fail-operate*. Associe:

sistemas que apresentam um estado seguro, geralmente não operacional, que pode ser alcançado modificando as saídas de atuadores (effectors) após detecção de falha	fail-safe
sistemas que para se manter em operação tolerando falhas aplicam redundância, como por exemplo, backups ou replicação de componentes	fail-operate
sistemas que devem permanecer em operação mesmo após detecção de falha em um ou mais de seus componentes	fail-operate

Correto

Notas relativas a este envio: 1/1.

Question15

Notas: 1

Considere os conceitos de sistemas *fail-safe* e sistemas *fail-operate*. Associe os exemplos ao termo:

sistemas de controle fly-by-wire	fail-operate
a maioria das aplicações de controle da vida-real	fail-safe
controle de uma ferramenta industrial de corte (guilhotina)	fail-safe

Correto

Notas relativas a este envio: 1/1.

Question16

Notas: 1

Relacionado ao texto sobre sistemas *fail-operate*, assinale verdadeiro e falso de acordo com as afirmações do autor.

Redundância de componentes é um conceito simples de fácil implementação.	Falso
Dunn afirma que sistemas fail-operate usam duas abordagens de tolerância a falhas: backup e replicação de componentes.	Verdadeiro
Os processos de detecção de falhas, isolamento e reconfiguração podem se tornar complexos aumentando muito os custos de desenvolvimento.	Verdadeiro
O uso de backups evita a degradação de desempenho em sistemas fail-operate, como no caso do Airbus A320.	Verdadeiro

Parcialmente correta

Notas relativas a este envio: 0.75/1.

Question17

Notas: 1

Para projetar um sistema fail-operate, Dunn menciona que os projetistas seguem normalmente dois métodos, que ele denomina *two-step* e *cut-and-try*. Associe as características listadas abaixo aos métodos:

Primeiro o projetista escolhe a arquitetura de hardware redundante e depois completa com os processos de gerência de redundância.	two-step
O projetistas iniciam com um projeto não redundante e incrementalmente incluem redundância e processos de gerenciamento de redundância até alcançar os objetivos.	cut-and-try
Método considerado impraticável pelo autor.	two-step

Correto

Notas relativas a este envio: 1/1.

Question18

Notas: 1

Dunn cita três técnicas analíticas que são usadas para determinar se os procedimentos aplicados para reduzir o risco de acidentes em um sistema alcançaram o nível de risco adequado. Marque com X as siglas que correspondem a essas três técnicas analíticas.

FMEA	X
IEC	-
FTA	X

MIL	-
SIL	-
RA	X

Correto

Notas relativas a este envio: 1/1.

Question19

Notas: 1

O projetista examina cada componente no sistema, considera como o componente pode apresentar defeito e então determina o efeito que cada defeito de componente pode provocar no sistema. O nome da técnica analítica sendo empregada é:

Escolher uma resposta.

○	a. RA ✗
○	b. cadeia de Markov ✗
○	c. FTA ✗
◉	d. FMEA ✓
○	e. IEC ✗
○	f. SIL ✗

Correto

Notas relativas a este envio: 1/1.

Question20
Notas: 1

A técnica analítica conhecida por análise de modos de defeito e efeitos procura principalmente verificar se existe algum ponto único de defeito no sistema que possa anular os benefícios da aplicação dos procedimentos de redução de riscos.

Correto
Notas relativas a este envio: 1/1.

Question21
Notas: 1

O projetista inicia com um acidente (*mishap*) identificável e trabalha retroativamente identificando todos os componentes que podem causar tal acidente e todos os dispositivos de segurança que podem evitá-lo. O nome da técnica analítica sendo empregada é:

Escolher uma resposta.

- a. SIL ✗
- b. cadeia de Markov ✗
- c. FTA ✓
- d. FMEA ✗
- e. IEC ✗
- f. RA ✗

Correto
Notas relativas a este envio: 1/1.

Question22
Notas: 1

Entre os técnicas analíticas citadas por Dunn, identifique os métodos qualitativos e os quantitativos.

FMEA	qualitativo
FTA	qualitativo
RA	quantitativo
DD	não citado no artigo
RBD	não citado no artigo

Correto

Notas relativas a este envio: 1/1.

Question23
Notas: 1

O analista deve determinar a probabilidade de defeito de cada componente na árvore de falhas. Os componentes são: de hardware, de software e operador. O resultado é numérico e geralmente fornecido como probabilidade de defeito por hora. O nome da técnica analítica sendo empregada é:

Escolher uma resposta.

- a. FTA ✗
- b. IEC ✗

○	c. SIL ✗
○	d. cadeia de Markov ✗
○	e. FMEA ✗
◉	f. RA ✓

Correto

Notas relativas a este envio: 1/1.

Question24

Notas: 1

A siglas Mil-Std-882D e IEC 61508, citadas por Dunn, correspondem a:

Escolher uma resposta.

○	a. bases de dados que fornecem a probabilidade de defeitos de componentes eletrônicos por hora ✗
○	b. métodos de cálculo quantitativos para determinação da confiabilidade de componentes ✗
◉	c. padrões na área de confiabilidade e segurança ✓
○	d. métodos qualitativos para determinação da probabilidade de defeitos de componentes de hardware e software ✗
○	e. leis internacionais que devem ser seguidas no projeto de hardware confiável ✗

Correto

Notas relativas a este envio: 1/1.

Question25
Notas: 1

Dunn afirma que enquanto um projeto não alcança o nível de risco adequado devem ser adotadas medidas para redução de risco. O que acontece tão logo o cálculo de risco do projeto indica que ele alcançou o nível de risco adequado?

Escolher uma resposta.

○	a. deve ser produzido e colocado em operação antes de se tornar obsoleto. ✗
○	b. deve ser documentado e ser solicitada a certificação por uma agência certificadora internacional. ✗
○	c. deve ser avaliado o custo de produção e tomada a decisão de comercialização ou abandono do projeto. ✗
◉	d. deve passar por validação adicional como verificação aprofundada de risco, testes e ensaios de campo. ✓

Correto

Notas relativas a este envio: 1/1.

Question26
Notas: 1

Assinale verdadeiro ou falso:

Para alcançar redução de risco, é exigido que todos os componentes de um sistema sejam considerados: hardware e software, sensores, atuadores, operador e a aplicação.	Verdadeiro
Dunn afirma que um acompanhamento rigoroso deve ser mantido durante toda a vida operacional de um sistema crítico para garantir que o risco de acidentes permaneça no, ou fique abaixo do, nível de risco obtido no projeto	Verdadeiro

original.

Dunn afirma que é óbvio que as preocupações do projetista sobre a segurança funcional (safety) de um sistema crítico se encerram quando termina o projeto e a implementação do sistema.

Falso

Correto

Notas relativas a este envio: 1/1.