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.