**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 |  |  |
| sensor de temperatura marcando temperatura abaixo da temperatura real da água |  |  |
| sobreaquecimento da água |  |  |
| a explosão do tanque de água causada pelo sobreaquecimento da água além do ponto de ebulição |  |  |
| a interface de hardware do computador comanda permanentemente "manter aquecimento" para a unidade de aquecimento de água |  |  |

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 Correto |  |
|  | b. escolher uma boa equipe de desenvolvedores Errado |  |
|  | c. aumentar a qualidade e a confiabilidade dos componentes Correto |  |
|  | d. usar ferramentas de desenvolvimento certificadas Errado |  |
|  | e. incorporar dispositivos de segurança externos Correto |  |

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) Correto |  |
|  | 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 Errado |  |
|  | c. zerar a probabilidade de ocorrência de defeitos Errado |  |
|  | d. eliminar as fontes que potencialmente causam defeitos de componentes Errado |  |

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 Errado |  |
|  | b. uso de componentes redundantes de software e hardware Correto |  |
|  | c. certificação do sistema pela IEC 61508 Errado |  |
|  | d. evitar problemas que resultam de condições ambientais impróprias Errado |  |
|  | e. reprojeto Errado |  |

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 Errado |  |
|  | b. defeitos elusivos Errado |  |
|  | c. defeitos maliciosos Errado |  |
|  | d. defeitos sistemáticos Correto |  |
|  | e. defeitos evasivos Errado |  |

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 Correto |  |
|  | b. abordagens baseadas em automação de projeto sem interferência humana Errado |  |
|  | c. evitar usar componentes de software Errado |  |
|  | d. abordagens orientadas a redundância Errado |  |
|  | e. reprojeto do sistema Errado |  |

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 Errado |  |
|  | b. quando se deseja reduzir os custos além de reduzir os riscos Errado |  |
|  | c. quando o projeto foi mal especificado e ninguém conhece como ele vai se comportar em operação real Errado |  |
|  | d. quando redundância se torna economicamente inviável Errado |  |
|  | e. quando o projeto requer passos adicionais para reduzir os riscos abaixo do nível de risco alcançado pelas medidas de qualidade e confiabilidade Correto |  |

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 Errado |  |
|  | b. uma barreira que evita a ocorrência de falhas de software e hardware Errado |  |
|  | c. uma barreira contra defeitos sistemáticos Correto |  |
|  | d. uma solução de baixo custo para evitar acidentes Errado |  |

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 Errado |  |
|  | b. dispositivos externos de segurança Correto |  |
|  | c. dispositivos especializados em segurança Errado |  |
|  | d. dispositivos de alta confiabilidade Errado |  |
|  | e. dispositivos redundantes Errado |  |

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 Errado |  |
|  | b. usar as 3 formas de redução de risco de forma balanceada e evitando negligenciar alguma parte do sistema Correto |  |
|  | c. enfatizar qualidade e confiabilidade dos componentes de hardware e software Errado |  |
|  | d. enfatizar dispositivos externos de segurança pois são mais baratos e eficientes que os demais recursos de segurança Errado |  |
|  | e. enfatizar dispositivos internos de segurança pois são mais baratos e eficientes que os demais recursos de segurança Errado |  |

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 |  |  |
| uso de uma chave de limitação de alta temperatura |  |  |
| componentes com confiabilidade superior aos usados em equipamentos convencionais |  |  |
| cuidados para garantir integridade estrutural do tanque de água |  |  |
| válvula de alívio de temperatura e pressão |  |  |

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 |  |  |
| detecta defeitos em atuadores realimentando a saída do atuador no computador para verificar se a saída corresponde ao comando enviado |  |  |
| inibe ação do atuador (effector) a menos que alguma condição física externa seja satisfeita |  |  |
| verifica a integridade do sistema de entrada e saída do computador |  |  |
| inibe as saídas do atuador (effector) forçando o sistema para um estado seguro |  |  |
| inibe a ação do atuador (effector) se o computador (ou o software) apresentar defeito e parar de enviar pulsos indicando que está em operação |  |  |

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 Errado |  |
|  | b. watchdog timer Errado |  |
|  | c. parada de emergência Errado |  |
|  | d. wraparound Errado |  |
|  | e. intertravamento Correto |  |

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 |  |  |
| sistemas que para se manter em operação tolerando falhas aplicam redundância, como por exemplo, backups ou replicação de componentes |  |  |
| sistemas que devem permanecer em operação mesmo após detecção de falha em um ou mais de seus componentes |  |  |

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 |  |  |
| a maioria das aplicações de controle da vida-real |  |  |
| controle de uma ferramenta industrial de corte (guilhotina) |  |  |

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

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. |  |  |
| O projetistas iniciam com um projeto não redundante e incrementalmente incluem redundância e processos de gerenciamento de redundância até alcançar os objetivos. |  |  |
| Método considerado impraticável pelo autor. |  |  |

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 |  |  |
| IEC |  |  |
| FTA |  |  |
| MIL |  |  |
| SIL |  |  |
| RA |  |  |

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 Errado |  |
|  | b. cadeia de Markov Errado |  |
|  | c. FTA Errado |  |
|  | d. FMEA Correto |  |
|  | e. IEC Errado |  |
|  | f. SIL Errado |  |

Correto

Notas relativas a este envio: 1/1.

Question20

Notas: 1

A técnica analítica conhecida por  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 Errado |  |
|  | b. cadeia de Markov Errado |  |
|  | c. FTA Correto |  |
|  | d. FMEA Errado |  |
|  | e. IEC Errado |  |
|  | f. RA Errado |  |

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 |  |  |
| FTA |  |  |
| RA |  |  |
| DD |  |  |
| RBD |  |  |

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 Errado |  |
|  | b. IEC Errado |  |
|  | c. SIL Errado |  |
|  | d. cadeia de Markov Errado |  |
|  | e. FMEA Errado |  |
|  | f. RA Correto |  |

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 Errado |  |
|  | b. métodos de cálculo quantitativos para determinação da confiabilidade de componentes Errado |  |
|  | c. padrões na área de confiabilidade e segurança Correto |  |
|  | d. métodos qualitativos para determinação da probabilidade de defeitos de componentes de hardware e software Errado |  |
|  | e. leis internacionais que devem ser seguidas no projeto de hardware confiável Errado |  |

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. Errado |  |
|  | b. deve ser documentado e ser solicitada a certificação por uma agência certificadora internacional. Errado |  |
|  | c. deve ser avaliado o custo de produção e tomada a decisão de comercialização ou abandono do projeto. Errado |  |
|  | d. deve passar por validação adicional como verificação aprofundada de risco, testes e ensaios de campo. Correto |  |

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. |  |  |
| 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 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. |  |  |

Correto

Notas relativas a este envio: 1/1.