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