9,0

Bacharelado em Ciência da Computação	
Disciplina: Modelos e Técnicas Computacionais para Análise de Requisitos de Segurança (Safety e Security)	
Valor: 10 pontos (peso 0.4)	**Data:** 26/05/2025
Professor: Rodrigo Martins Pagliares	

Gabarito: Agradeço se você puder repassar suas respostas para quadro abaixo. Isso facilita durante minha correção.

1	2	3	4	5	6	7	8	9	10
E	D	A	A	C	C	E	C	D	B
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
A	A	B	C	E	D	E	B	C	E

1. Assinale a alternativa CORRETA sobre a diferença entre requisitos de *safety* e de *security*:

a) Requisitos de *safety* buscam garantir a confidencialidade de dados sensíveis, enquanto requisitos de *security* asseguram que o sistema permaneça em operação sem interrupções.
b) Requisitos de *safety* são mais relevantes do que os de *security*, especialmente em sistemas que envolvem vidas humanas.
c) Requisitos de *security* são formulados exclusivamente para ambientes financeiros e transacionais.
d) Ambos os tipos de requisitos se referem às características de desempenho computacional, como tempo de resposta e latência.
e) Requisitos de *safety* têm como foco a prevenção de perdas que causem danos físicos, operacionais ou ambientais; requisitos de *security* lidam com a proteção contra ameaças intencionais que comprometam a integridade, disponibilidade ou confidencialidade do sistema.

2. Assinale a alternativa CORRETA sobre as diferenças entre "perda" (*loss*) e "perigo" (*hazard*) na STPA:

a) Perda é causada por falhas físicas de componentes, enquanto perigo representa a falha de comunicação entre subsistemas de *software*.
b) Perda corresponde diretamente a um acidente registrado; perigo é o mesmo que probabilidade de ocorrência.
c) Perigo é definido como um tipo específico de falha elétrica que compromete o funcionamento do sistema; perda é a consequência ambiental do evento.
d) Perda é um resultado indesejado para o sistema ou seus usuários; perigo é uma condição ou estado que pode levar à ocorrência dessa perda. √
e) Os termos são usados como sinônimos na STPA e se referem às consequências de eventos operacionais inesperados. ×

3. Assinale a alternativa CORRETA sobre a especificação de requisitos:

a) Refere-se ao processo de documentação clara e consistente dos requisitos, com o objetivo de facilita a comunicação entre as partes envolvidas e permitir rastreabilidade.
b) Deve ser estruturada de forma a evitar validações posteriores, priorizando o ganho de tempo no processo de desenvolvimento.
c) Em métodos ágeis, a formalização dos requisitos é desnecessária, já que o processo se baseia em comunicação direta.
d) Atua como substituta da fase de elicitação, uma vez que os requisitos já são conhecidos antes da análise do sistema.
e) É uma atividade complementar que pode ser realizada após a implementação, com base nos testes realizados.

4. Assinale a alternativa CORRETA sobre modelos mentais no contexto da STPA:

a) Têm como principal função representar as respostas esperadas dos sensores a estímulos do ambiente físico.
b) Correspondem a comandos automáticos executados diretamente por dispositivos de controle baseados em *hardware*.
c) São abstrações técnicas que substituem diretamente os algoritmos implementados em sistemas embarcados.
d) Refletem a forma como controladores humanos percebem, interpretam e antecipam o comportamento do sistema, influenciando suas decisões.
e) São considerados subjetivos e, por isso, não devem ser incluídos formalmente nas análises de sistemas complexos.

5. Assinale a alternativa CORRETA sobre requisitos funcionais:

a) Referem-se aos aspectos visuais e de apresentação do sistema, como *layout*, cores e estilo da interface.
b) Estabelecem regras de operação com foco em atributos de desempenho e confiabilidade sob diferentes condições de carga.
c) Descrevem as funcionalidades específicas e os comportamentos que o sistema deve executar para atender às necessidades dos usuários.
d) Incluem definições de componentes físicos e limitações de infraestrutura tecnológica que afetam a arquitetura do sistema.
e) Relacionam-se a obrigações contratuais ou normativas, como leis e regulamentações que impactam o desenvolvimento do software.

6. Assinale a alternativa CORRETA sobre os tipos de ações de controle inseguras (UCAs) identificadas na STPA:

a) São geralmente associadas à falha de sensores que enviam sinais incorretos ao sistema de controle.
b) Compreendem ações de controle que não são fornecidas quando deveriam, são fornecidas quando não deveriam, ocorrem em momentos inadequados ou têm duração inadequada.
c) Estão ligadas a situações em que a sequência esperada de comandos é violada por um erro de execução.
d) Dizem respeito a instruções que exigem a ativação de componentes físicos com potencial de gerar impacto mecânico direto.
e) Estão normalmente relacionadas a quedas de energia que impedem o envio contínuo de comandos.

Assinale a alternativa CORRETA sobre *stakeholders*:

a) Incluem exclusivamente os usuários finais, pois são os únicos afetados diretamente pelo funcionamento do sistema.
b) Englobam atores externos ao projeto que atuam em mercados concorrentes ou setores regulatórios.
c) Dizem respeito prioritariamente aos financiadores do projeto, que exercem controle sobre os prazos e orçamento.
d) Compreendem os membros da equipe técnica, responsáveis por projetar, implementar e testar o sistema.
e) Abrangem qualquer indivíduo, grupo ou organização com interesse legítimo nas decisões, resultados ou operação do sistema, seja de forma direta ou indireta.

8. Assinale a alternativa CORRETA sobre controladores humanos na STPA:

a) São considerados elementos externos ao sistema analisado e, por isso, não são incluídos na modelagem da estrutura de controle.
b) Costumam ser ignorados devido à dificuldade de prever o comportamento humano em sistemas complexos.
c) São tratados como controladores ativos, com responsabilidades, modelos mentais e interações que influenciam diretamente o comportamento do sistema.
d) São documentados apenas por meio de diagramas descritivos, sem representação funcional na estrutura de controle.
e) Precisam ser substituídos por mecanismos automáticos para garantir consistência na análise de riscos.

9. Assinale a alternativa CORRETA sobre requisitos de *security*:

a) Estão voltados à integridade física dos operadores e à prevenção de acidentes decorrentes de interação humana com o sistema.
b) Focam na resistência mecânica de componentes e na minimização de falhas técnicas por desgaste ou sobrecarga.
c) São definidos principalmente para aplicações sensíveis, como sistemas hospitalares e financeiros, onde a segurança da informação é considerada prioritária.
d) Estabelecem mecanismos para proteger o sistema contra acessos não autorizados, alterações indevidas e falhas de disponibilidade, cobrindo aspectos de confidencialidade, integridade e disponibilidade.
e) Estão relacionados a preferências estéticas, responsividade da interface e percepção subjetiva de facilidade de uso por parte do usuário final.

10. Assinale a alternativa CORRETA sobre os modelos de processo inadequados:

a) Estão associados a erros estatísticos em cálculos de otimização utilizados em sistemas adaptativos.
b) Representam situações em que o controlador age com base em informações incompletas ou incorretas sobre o estado do sistema.
c) Referem-se a defeitos físicos em subsistemas de energia que causam interrupções operacionais.
d) Ocorrências desse tipo são características exclusivas de sistemas legados com baixa atualização tecnológica.
e) Afetam apenas a documentação técnica do sistema, sem alterar seu comportamento real.

11. Assinale a alternativa CORRETA sobre prototipagem:

a) Facilita o entendimento dos requisitos por parte dos *stakeholders*, servindo como apoio visual e interativo ao processo de elicitação.
b) Substitui completamente a necessidade de registrar os requisitos de forma estruturada e verificável.
c) Funciona como alternativa à documentação tradicional e elimina a necessidade de validação formal.
d) Aplica-se apenas a projetos que envolvem interfaces gráficas detalhadas e interação direta com o usuário final.
e) Deve ser evitada em interações com *stakeholders* para manter a objetividade da análise.

12. Assinale a alternativa CORRETA sobre ações de controle na STPA:

a) São comandos emitidos pelos controladores com o objetivo de influenciar diretamente o comportamento do processo controlado.
b) Qualquer ação de controle enviada pelo sistema gera automaticamente uma situação de risco.
c) Representam instruções executadas pelos atuadores em resposta a eventos externos.
d) Correspondiam a sinais de entrada gerados espontaneamente pelos sensores em sistemas reativos.
e) São consideradas comunicações passivas sem impacto direto na operação do sistema.

13. Assinale a alternativa CORRETA sobre ferramentas de requisitos:

a) Devem ser integradas apenas no final do desenvolvimento, quando os requisitos já estiverem estabilizados.
b) Auxiliam na organização, rastreamento e controle das alterações dos requisitos ao longo do ciclo de vida do projeto.
c) Tornam desnecessárias as interações presenciais com a equipe durante a coleta e validação de requisitos.
d) São projetadas para uso exclusivo por profissionais da área de testes de software.
e) Têm pouca utilidade em projetos de pequeno porte, devido à sua complexidade operacional.

14. Assinale a alternativa CORRETA sobre falhas de execução de ações de controle:

a) São consideradas irrelevantes no contexto da STPA, pois essa técnica prioriza apenas falhas de concepção.
b) Estão limitadas a erros cometidos por operadores humanos durante a interação com o sistema.
c) Ocorrem quando uma ação de controle é enviada corretamente, mas não é implementada de forma eficaz no processo controlado.
d) São neutras em termos de impacto, desde que o sistema esteja operando com energia e redundância ativa.
e) Resultam exclusivamente de falhas de lógica em algoritmos de controle e não envolvem aspectos físicos.

15. Assinale a alternativa CORRETA sobre o conceito de *Capability Gap*:

a) Refere-se à trajetória histórica de um requisito desde sua criação até a remoção.
b) Designa o conjunto de funcionalidades mantidas por sistemas legados sem atualização.
c) Está associado ao planejamento e execução de testes de regressão em ciclos de desenvolvimento contínuo.
d) Trata-se de um tipo especial de requisito de usabilidade vinculado à experiência do usuário.
e) É a diferença identificada entre a capacidade atual de um sistema e a capacidade necessária para atender aos objetivos definidos.

Assinale a alternativa CORRETA sobre como os resultados da STPA podem ser utilizados:

a) São úteis para fins investigativos após acidentes, mas não influenciam decisões de projeto preventivas.
b) Direcionam a criação de testes de *software* de baixo nível, focados em coberturas estruturais do código.
c) Servem como documentação complementar exigida por órgãos de auditoria, sem impacto direto na engenharia de sistemas.
d) Fornecem subsídios para definição de requisitos, orientações para arquitetura e recomendações de melhoria no projeto.
e) Substituem a modelagem comportamental baseada em notações como diagramas UML.

17. Assinale a alternativa CORRETA sobre o conceito de *requirements scrubbing*:

a) Envolve a remoção completa de todos os requisitos que ainda não foram formalmente aprovados.
b) Foca na identificação de *stakeholders* que possam estar em desacordo com os objetivos do sistema.
c) Consiste em eliminar qualquer tipo de requisito que apareça mais de uma vez no documento técnico.
d) Serve como alternativa à fase de testes de integração, reduzindo a necessidade de validação cruzada.
e) Tem como finalidade selecionar e refinar o conjunto de requisitos mais consistente e viável para implementação.

18. Assinale a alternativa CORRETA sobre a inclusão de cenários com adversários:

a) Não são considerados na STPA, pois essa técnica se aplica apenas à análise de acidentes não intencionais.
b) São incluídos para considerar falhas induzidas por agentes maliciosos, como falsificação de sinais (*spoofing*) ou alteração de comandos.
c) Devem ser avaliados exclusivamente após a fase de implementação e testes de segurança.
d) São tratados como riscos externos que não precisam ser modelados dentro da estrutura funcional do sistema.
e) São mapeados separadamente do processo de análise de perda, já que envolvem ameaças intangíveis.

19. Assinale a alternativa CORRETA sobre requisitos ambíguos:

a) Podem ser desejáveis em projetos experimentais, pois oferecem espaço para interpretações múltiplas.
b) Favorecem a produtividade da equipe ao permitir liberdade de implementação.
c) Aumentam o risco de entregar um sistema que não atende às necessidades reais dos usuários ou *stakeholders*.
d) Contribuem para facilitar ajustes futuros no escopo sem necessidade de revalidação.
e) Auxiliam na identificação de otimizações durante a fase de codificação.

20. Assinale a alternativa CORRETA sobre a finalidade geral da STPA:

a) Substituir completamente métodos baseados em confiabilidade estatística na engenharia de sistemas críticos.

b) Localizar falhas raras de componentes que geram eventos isolados com impacto operacional limitado.

c) Avaliar apenas falhas de dispositivos eletrônicos, negligenciando fatores humanos e organizacionais.

d) Validar a conformidade da arquitetura do sistema com normas específicas, como a ISO 26262.

(e) Identificar condições inseguras que podem levar a perdas, mesmo quando todos os componentes do sistema funcionam corretamente.

Boa Prova !
Rodrigo Martins Pagliares