

Análise de Falhas e Causas

Atividade: Lab01 - GQS

Aluno: Pedro Zorzete / **RA:** 823147399

Professor: Robson Calvetti / **Disciplina:** Gestão e Qualidade de Software – GQS

Ariane 5 (1996)

Falha	Causa	Prevenção
Explosão do foguete Ariane 5 poucos segundos após o lançamento.	Erro de conversão numérica (overflow), tentativa de converter um valor de 64 bits em 16 bits no código reutilizado do Ariane 4.	Revisão de requisitos considerando novos limites de operação; testes de simulação com cenários extremos; auditoria independente de software reutilizado.

Ligação com ISO/IEC 25010 – Qualidade de Produto

O caso está relacionado à característica de **confiabilidade**. A falha demonstrou ausência de consistência sob condições operacionais novas, comprometendo o desempenho esperado.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Área de processo afetada: Gestão de Configuração (CM) e Verificação (VER) = houve reuso de código sem controle formal de versão e sem verificação em novos contextos.

Importância dos Testes e Auditorias

Testes de integração e regressão teriam identificado o overflow antes do lançamento. Auditorias independentes também evitariam o reuso inseguro do código.

Papel da Gestão de Requisitos

Os requisitos deveriam prever limites numéricos compatíveis com a nova arquitetura e exigir validação sob condições de voo reais.

Therac-25 (anos 80)

Falha	Causa	Prevenção
Pacientes expostos a doses letais de radiação em um acelerador de partículas.	Erro no software que controlava a posição da placa metálica; ausência de verificação e testes independentes.	Revisão de código independente, redundância de sistemas, validação de requisitos críticos e treinamento dos operadores.

Ligação com ISO/IEC 25010 – Qualidade de Produto

Relaciona-se à **segurança** pois o sistema não oferece proteção contra falhas perigosas e não garante a integridade do usuário.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Áreas de processo: Gerência de Requisitos (REQM) e Validação (VAL) = falhou em definir e validar requisitos críticos de segurança.

Importância dos Testes e Auditorias

Testes de verificação formal e simulação de cenários extremos evitariam a exposição à radiação. Auditorias de código e requisitos detectaram lacunas de segurança.

Papel da Gestão de Requisitos

Os requisitos deveriam incluir intertravamentos físicos e lógicos obrigatórios, rastreabilidade e validação clínica antes da produção.

Bug do Ano 2000 (Y2K)

Falha	Causa	Prevenção
Sistemas interpretaram o ano 2000 como 1900, podendo causar falhas em larga escala.	Anos armazenados com dois dígitos; falta de previsão e dependência de sistemas legados.	Atualização e auditoria de sistemas, padronização para quatro dígitos, testes simulando transição de datas e planos de contingência.

Ligação com ISO/IEC 25010 – Qualidade de Produto

Relaciona-se à **Compatibilidade e Eficiência de Desempenho** pois há a falta de compatibilidade temporal entre versões de sistemas e erros de cálculo em operações baseadas em datas.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Áreas de processo: Gestão de Riscos (RSKM) e Gestão de Configuração (CM = Falha na antecipação e controle de riscos de longo prazo.

Importância dos Testes e Auditorias

Testes de regressão e simulação de datas futuras teriam detectado o erro. Auditorias de sistema teriam identificado dependências críticas.

Papel da Gestão de Requisitos

Os requisitos deveriam especificar armazenamento de datas com quatro dígitos e prever evolução tecnológica ao longo do tempo.

Knight Capital (2012)

Falha	Causa	Prevenção
Erro em sistema de negociação causou perda de US\$440 milhões em 45 minutos.	Deploy de software mal testado, conflito entre módulos novos e antigos.	Testes rigorosos antes de deploy, validação de compatibilidade, monitoramento em tempo real e plano de reversão rápida.

Ligação com ISO/IEC 25010 – Qualidade de Produto

Relaciona-se à **Confiabilidade e Manutenibilidade**, comportamento inconsistente e código legado não removido adequadamente.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Áreas de processo: Verificação (VER) e Gerência de Configuração (CM) = ausência de testes formais e falha no controle de versões.

Importância dos Testes e Auditorias

Testes de integração e regressão teriam revelado conflitos entre módulos. Auditorias de deploy preveniriam ativação de código obsoleto.

Papel da Gestão de Requisitos

Os requisitos deveriam incluir rollback automático, controle de versões e contingência operacional para sistemas financeiros críticos.

Toyota (2009–2011)

Falha	Causa	Prevenção
Aceleração involuntária em veículos, causando acidentes e recalls.	Bug no software do sistema eletrônico de controle do acelerador (ETCS), falhas de integração entre software e mecânica.	Revisão rigorosa de software embarcado, testes de integração e gestão proativa de recalls.

Ligação com ISO/IEC 25010 – Qualidade de Produto

Relaciona-se à **Segurança e Usabilidade** pois o sistema não forneceu resposta previsível e segura ao usuário final.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Áreas de processo: Validação (VAL) e Gerência de Requisitos (REQM) = requisitos críticos de segurança não validados adequadamente.

Importância dos Testes e Auditorias

Testes de integração e stress em ambiente real evitariam falhas de aceleração. Auditorias de segurança garantiriam redundância.

Papel da Gestão de Requisitos

Os requisitos deveriam prever respostas seguras a falhas de sensor, redundância e limites de aceleração controlados por software.

Uber (2022)

Falha	Causa	Prevenção
Invasão hacker compromete sistemas internos após ataque de MFA fatigue.	Funcionário aprovou autenticações múltiplas; falta de bloqueio automático e treinamento em segurança.	Educação contínua, limitação de tentativas de MFA, auditoria de acessos e monitoramento proativo.

Ligação com ISO/IEC 25010 – Qualidade de Produto

Relaciona-se à **Segurança** pois a vulnerabilidade em autenticação multifatorial e controle de acessos.

Ligação com CMMI/MPS.BR – Qualidade de Processo

Áreas de processo: Gestão de Riscos (RSKM) e Verificação (VER) = falta de mitigação e monitoramento de riscos de segurança.

Importância dos Testes e Auditorias

Testes de penetração e auditorias de segurança evitariam o ataque. Revisões de políticas de MFA reduziram vulnerabilidades.

Papel da Gestão de Requisitos

Os requisitos deveriam especificar limites de autenticação, alertas automáticos e monitoramento de tentativas suspeitas.