Etec de São Paulo

Desenvolvimento de Sistemas

Especificação e desenvolvimento de sistemas críticos

São Paulo

2021

Etec de São Paulo

Desenvolvimento de Sistemas

Especificação e desenvolvimento de sistemas críticos

Nomes:

Hertz Franz Bancher

José Felipe Higino Araújo

Rafael Bismark Flores Zarate

Rodrigo Cotrin Guimarães da Silva

Sophia Albuquerque Lima

Orientador: Luiz Ricardo de Souza

São Paulo

2021

Sumário

Introdução

Um computador precisa de instruções para funcionar, independentemente do seu tipo. É necessária uma linguagem legível por humanos que possa ser interpretada por máquinas. É definido como um conjunto de regras sintáticas e semânticas criadas para a construção de programas. Ele lê, executa, processa, transmite e ou armazena os resultados dessas instruções. Atualmente, existem vários paradigmas e linguagens de programação, cada um com características diferentes. Desta forma, programadores e engenheiros podem construir programas (aplicativos) organizados, rápidos e eficientes para realizar as tarefas esperadas. Às vezes, esses códigos são traduzidos para outra linguagem e, finalmente, compilados em uma sequência lógica compreensível pela máquina. Diz-se que se trata de um sistema crítico e, se falhar, pode causar danos materiais e ambientais, além de morte ou ferimentos graves.

Sistemas críticos

As falhas de software estão se tornando mais frequentes. Na maioria dos casos, os sistemas críticos causarão interrupções, causando perdas econômicas, danos físicos ou ameaças aos seres humanos. Alguns exemplos de interrupções:

washingtonpost.com > Technology > Special Reports > Cyber-Security

Cyber Incident Blamed for Nuclear Power Plant Shutdown

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

Network News PROFILE

View More Activity

TOOLBOX

Resize Print

E-mail Reprints

Sponsored Links

2014 Best Skin Tighteners

http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html

Software Bug Triggered Airplane Dive Emergency

When an airplane system monitoring Airbus jet's altitude and position output incorrect data, flight computers failed to compensate.

Investigators have released their final report into a 2008 Qantas flight QF72 from Singapore to Perth, Australia, in which 110 people were injured after a computer component failed. Interestingly, investigators have now found that a programming error was partly to blame for the incident.

Here's what happened: On October 7, 2008, aircraft-monitoring systems in the Airbus A330-303--flying at 37,000 feet--failed, causing the autopilot to automatically disconnect. But pilots were still at the mercy of a flight computer that was receiving incorrect data.

Roughly two minutes after the failure of the computer component, the flight computer initiated two deep dives, the first for 20 seconds, the second for 16 seconds. Each dive slammed passengers into ceilings and walls. Dozens of alarms, most of them false, also began sounding in the cockpit. Luckily, pilots were able to switch to fully manual controls and execute an emergency landing at a nearby Australian military base.

http://www.darkreading.com/risk-management/software-bug-triggered-airplane-dive-emergency/d/d-id/1101952?

TECH 8/19/2013 @ 3:50PM | 15.316 views

Amazon.com Goes Down, Loses $66,240 Per Minute

+ Comment Now + Follow Comments

It's been a bad week for ecommerce. On Friday, Google GOOG -1.01% temporarily went dark, causing a 40% drop in web traffic. Today Amazon.com AMZN -0.22% went down for approximately 30 minutes, preventing shoppers from accessing the site via Amazon.com, mobile and Amazon.ca.

amazon.com.

http://www.forbes.com/sites/kellyclay/2013/08/19/amazon-com-goes-down-loses-66240-per-minute/

O sistema crítico são sistemas sociotécnica ou técnico em que as pessoas dependem. Os sistemas críticos são definidos como um tipo de software cujas características causam riscos inerentes de perdas físicas, pessoais e financeiras. Atualmente, existem três tipos de sistemas principais, como:

- Sistema crítico de segurança: sua falha pode proceder em prejuízos, danos ambientais e perda da vida humana. Um exemplo de sistema crítico de segurança é um software de controle de uma fábrica de fogos de artifício.
- Sistema crítico de missão: sua falha pode ocasionar problema em alguma atividade conduzida a metas. Um exemplo de sistema crítico de missão é um software de navegação para uma aeronave.
- Sistema crítico de negócio: sua falha pode resultar em custos elevados para a empresa que trabalha com o software. Um exemplo de sistema crítico de negócio é um software contábil de clientes bancários.

Um sistema considerado crítico, precisa ser de total confiança. Há diversas razões para que a confiança seja de fundamental importância, tais como:

- Sistemas não confiáveis ou desprotegidos: se as pessoas não confiam nele, com certeza não vão querer utilizá-los.
- Custos de falhas nos sistemas são elevados: os custos de falhas nos softwares são altíssimos.

- Sistemas que levam a desconfiança ocasionam perdas de informações: as perdas de informações são ocorridas nesses softwares e podem ocasionar prejuízos enormes.

Devido o alto custo nas falhas dos sistemas críticos, eles são, na maioria das vezes, desenvolvidos com técnicas já conhecidas. Essas técnicas, embora antigas, tem seu ponto forte e fraco já conhecido, mas, ainda há componentes nos quais as falhas podem ocorrer, como exemplo menciona-se: o hardware do software pode falhar; pode ocorrer erros na especificação, projeto ou implementação e falhas humanas na operação do software.

Em um sistema crítico é preciso focar em todos os aspectos dele, como: hardware, software e processos operacionais, uma vez que qualquer falha pode acarretar problemas graves no futuro. Além disso, é preciso pensar também, na confiança, já que ela é fundamental no sistema considerado crítico.

Especificação Dirigida a Sistemas Críticos

<table>
<tr><th>Componentes
Categoria</th><th colspan="2">Desempenho</th><th>Suporte</th><th>Custo</th><th>Cronograma</th></tr>
<tr><td rowspan="2">Crítico</td><td>1</td><td colspan="2">Falha em atender o requisito degradará o desempenho do sistema até um ponto no qual o sucesso da missão é questionável</td><td colspan="2">Falha resulta em atrasos operacionais e/ou aumento de custos com valores estimados entre $ 100 mil e $ 500mil</td></tr>
<tr><td>2</td><td>Alguma redução no desempenho técnico</td><td>Pequenos atrasos nas modificações de software</td><td>Alguma falta de recursos financeiros, possíveis estouros de orçamento</td><td>Possível atraso na data de entrega</td></tr>
</table>

Especificar sistemas críticos é complicado, pois os riscos devem ser compreendidos e os requisitos de confiabilidade para lidar com eles devem ser gerados. As especificações para sistemas críticos envolvem alguns fatores, são eles:

- Análise e classificação de riscos: é preciso fazer uma análise para ver se determinado risco é uma ameaça ao ambiente ou ao sistema. Além disso, é preciso também, identificar os tipos de riscos, como: intolerável (riscos que ameaçam a vida humana ou a estabilidade financeira de um negócio), muito baixo (riscos que tem consequências mínimas) e aceitável (riscos que tem como ocorrência aceitável).

- Decomposição de riscos: é nesse processo em que descobre as origens dos riscos no software. São várias as técnicas propostas para a decomposição de riscos, e, como exemplo tem-se a análise de árvore de defeito (envolve a identificação do evento não desejado e a análise retroativa a partir desse evento, a fim de desmembrar as causas do risco).
- Avaliação de redução de riscos: ao identificar os riscos e as suas origens, é preciso derivar os requisitos de confiabilidade do software. Eles gerenciam os riscos e assegura que os acidentes não mais ocorram, mas, para isso, é preciso usar as seguintes estratégias: prevenção, detecção, remoção de riscos e limitação de danos.

Combinações de fatores são de fundamental importância em um sistema crítico, e, no entanto, cabe ao especificador se adequar as necessidades de cada sistema crítico.

Métodos de desenvolvimento para sistemas críticos

Os custos com falha de sistema crítico são tão altos que os métodos de desenvolvimento podem ser usados, embora não sejam eficazes em termos de custo para outros tipos de sistema. Exemplos de métodos de desenvolvimento:

• Métodos formais de desenvolvimento de software

• Análise estática

• Garantia de qualidade externa

Conclusão

Então podemos concluir que os sistemas críticos são essenciais para o ser humano atuando em diversas áreas e nos mais diversos setores como por exemplo na aviação, agronegócio e o mercado financeiro. Nesses sistemas podemos ver que a confiabilidade do usuário é fundamental para o seu funcionamento e usabilidade, pois se um sistema não é confiável as pessoas não vão usá-lo, causando assim grandes prejuízos para os criadores desse sistema.

Os cuidados a terem-se durante o desenvolvimento com sistemas críticos são muito a mais do que em outros sistemas, qualquer falha interfere na vida de alguém, podendo ferir, ou em pior dos casos matar alguma pessoa. Existe uma grande variedade de sistemas que são considerados críticos e devemos nos atentar durante a produção deles, desde à especificação ao desenvolvimento. A qualidade de um sistema crítico muita das vezes deve beirar a perfeição, por isso devemos estar preparados para todas as adversidades durante o projeto, cientes de que muitas coisas estão em jogo.

Referências Bibliográficas

Data de acesso: em 25/05/2021 (17:00)

https://www.devmedia.com.br/sistemascriticos/18952#:~:text=Os%20sistemas%20considerados%20cr%C3%ADticos%20precisam,confiabilidade%20para%20lidar%20com%20eles

Data de acesso: em 02/07/2021 (13:00)

https://pplware.sapo.pt/informacao/sistemas-criticos-e-ada/

http://disciplinas.lia.ufc.br/es10.1/arquivos/CAP03-resumo.pdf

Data de acesso: em 15/07/2021 (18:00)

https://www.cin.ufpe.br/~kiev/IF682/03_SistemasCriticos.pdf

Artigo:

Data de acesso: em 17/07/2021 (13:00)

https://www.revistauniversitas.inf.br/index.php/UNIVERSITAS/article/viewFile/217/145

Livro:

Data de acesso: 17/07/2021 (17:00)

PRESSMAN, R. S.. Engenharia de Software, McGraw-Hill, 7ª ed., 2011.

Sommerville - Engenharia de Software - 8ª ed