Qualidade de Software

Prof. Ms. Gustavo Molina

Aula 05 – Sistemas Críticos

msc.gustavo.unip@gmail.com

Sistemas Críticos

- ✓ **Sistemas críticos de segurança**

  A falha pode resultar em perda de vida, prejuízo ou dano para o ambiente;

  Sistema de proteção de plantaquímica.

- **Sistemas críticos de missão**

  A falha pode resultar na deficiência de alguma atividade dirigida a metas;

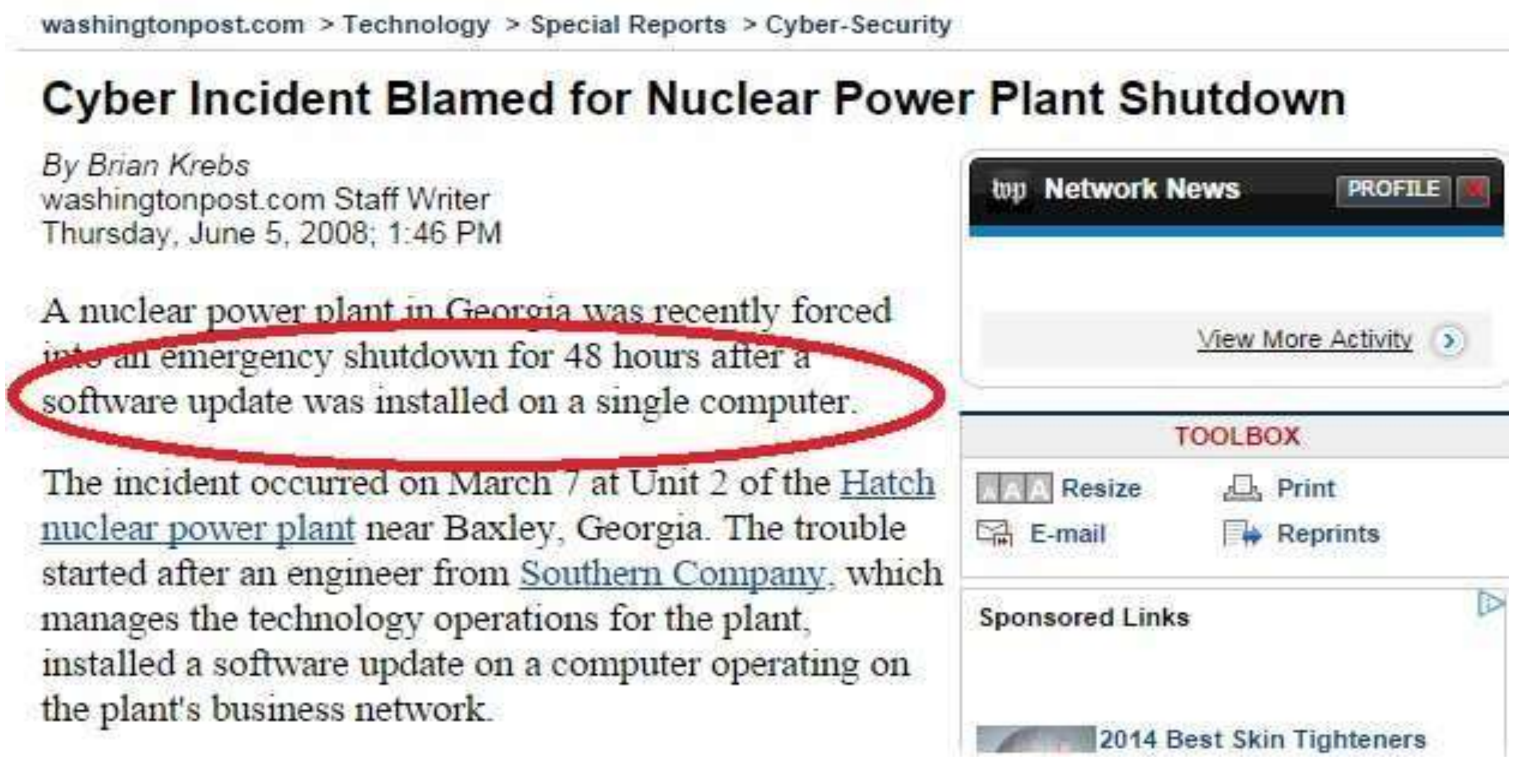
  Sistema de navegação de nave espacial.

- **Sistemas críticos de negócios**

  A falha pode resultar em altas perdas econômicas;

  Sistema de contas de cliente em um banco.

Sistemas Críticos



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

Cyber Incident Blamed for Nuclear Power Plant Shutdown

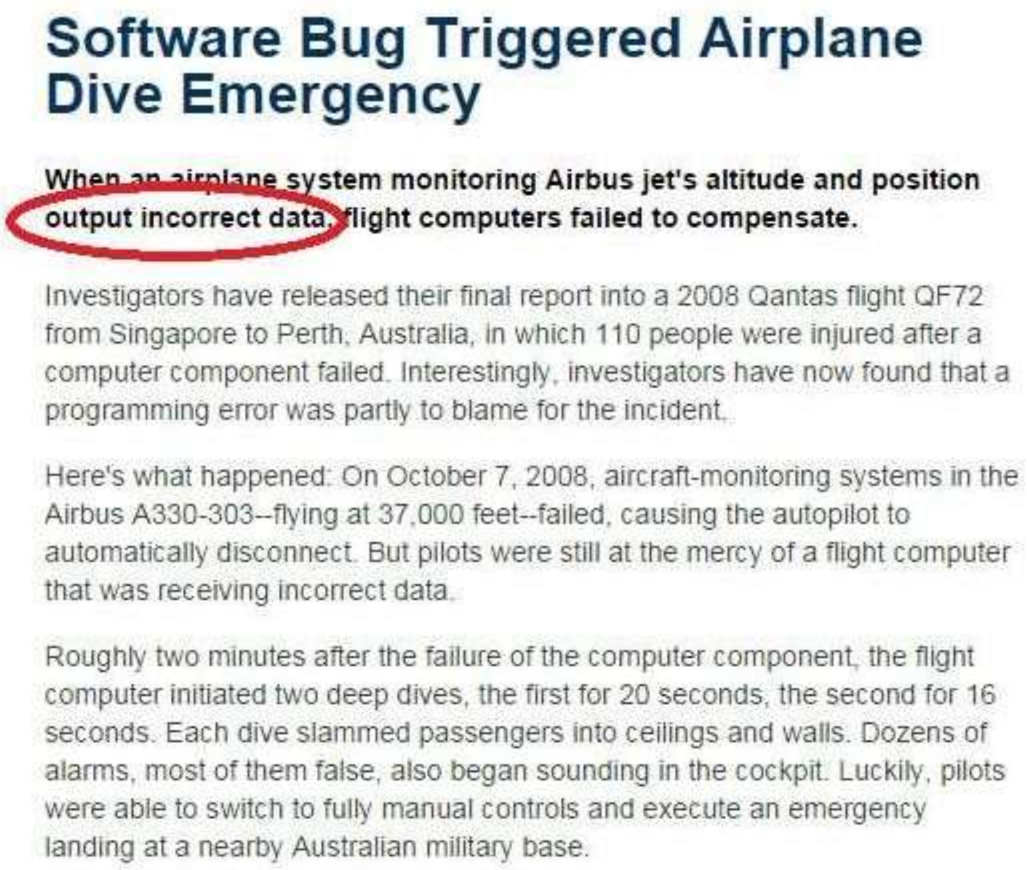
By Brian Krebs
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

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.

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

Sistemas Críticos



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.

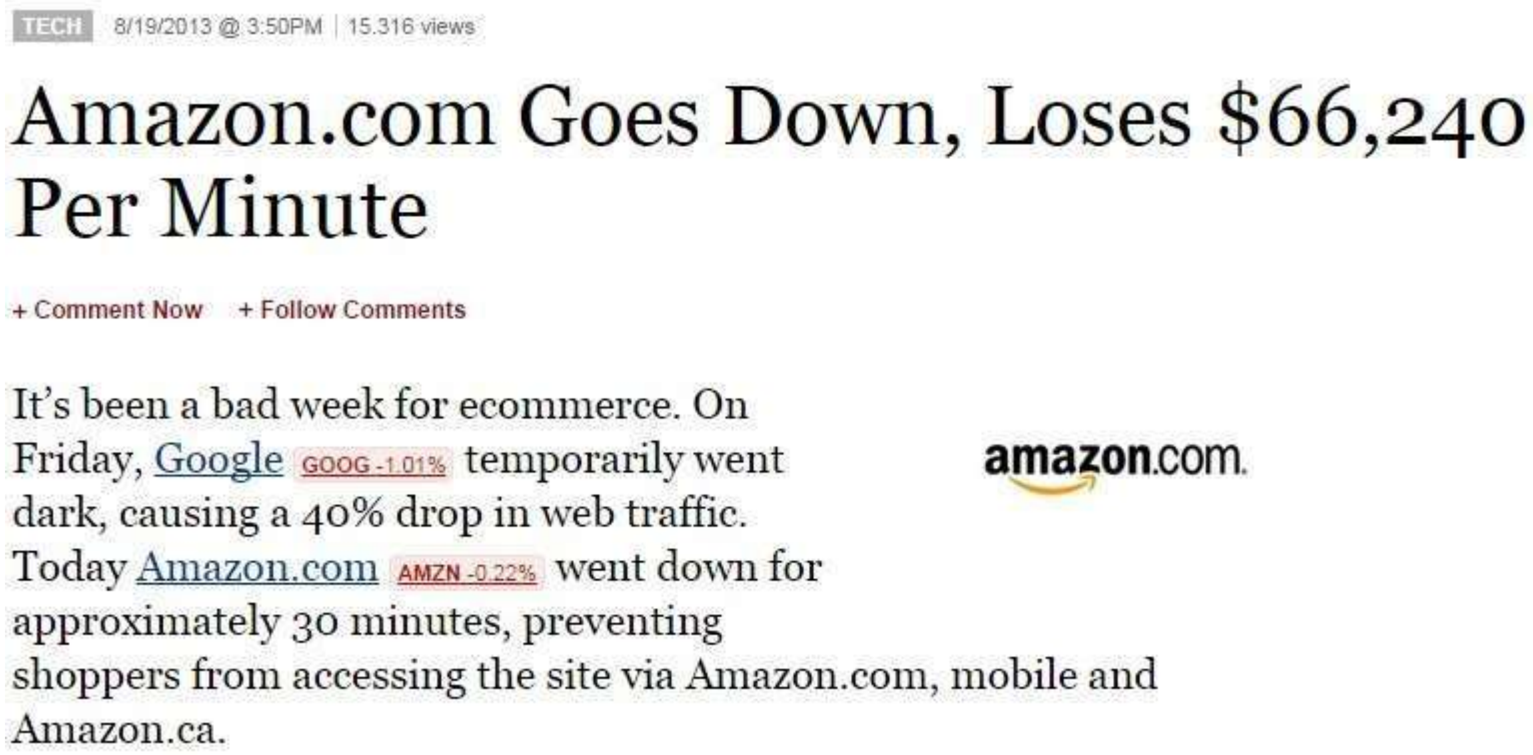
Investigators have released their final report into a 2008 Qantas flight QF72 from Singapore to Perth, Australia, in which 110 people were injured after a computer component failed. Interestingly, investigators have now found that a programming error was partly to blame for the incident.

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?

Sistemas Críticos



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.

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

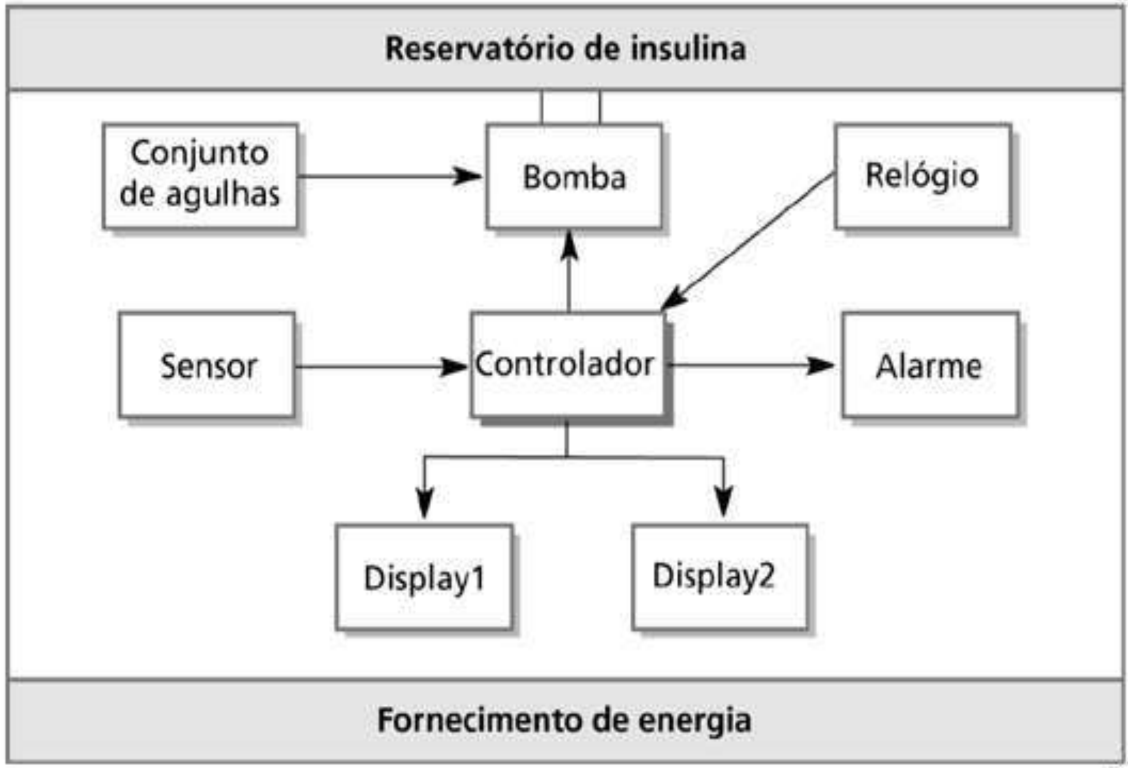
Uma Bomba de Insulina Controlada por Software

- Usada por diabéticos para simular a função do pâncreas, que produz insulina, um hormônio essencial que com a função de metabolizar o açúcar do sangue.
- Mede a glicose do sangue (açúcar) usando um micro sensor e calcula a dose de insulina necessária para metabolizar a glicose.

Organização da Bomba de Insulina

Figura 3.1

Estrutura de bomba de insulina



Fluxo de Dados da Bomba de Insulina

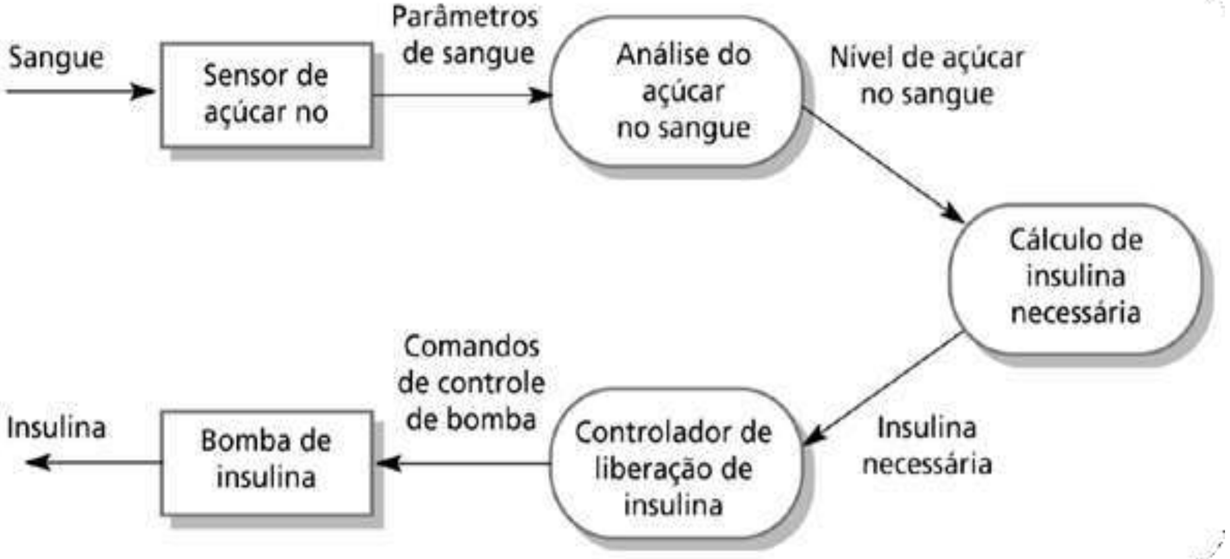

Sangue
Sensor de açúcar no
Parâmetros de sangue
Análise do açúcar no sangue
Nível de açúcar no sangue
Cálculo de insulina necessária
Insulina necessária
Controlador de liberação de insulina
Comandos de controle de bomba
Bomba de insulina
Insulina

Figura 3.2

Modelo de fluxo de dados de bomba de insulina

Requisitos de Confiança

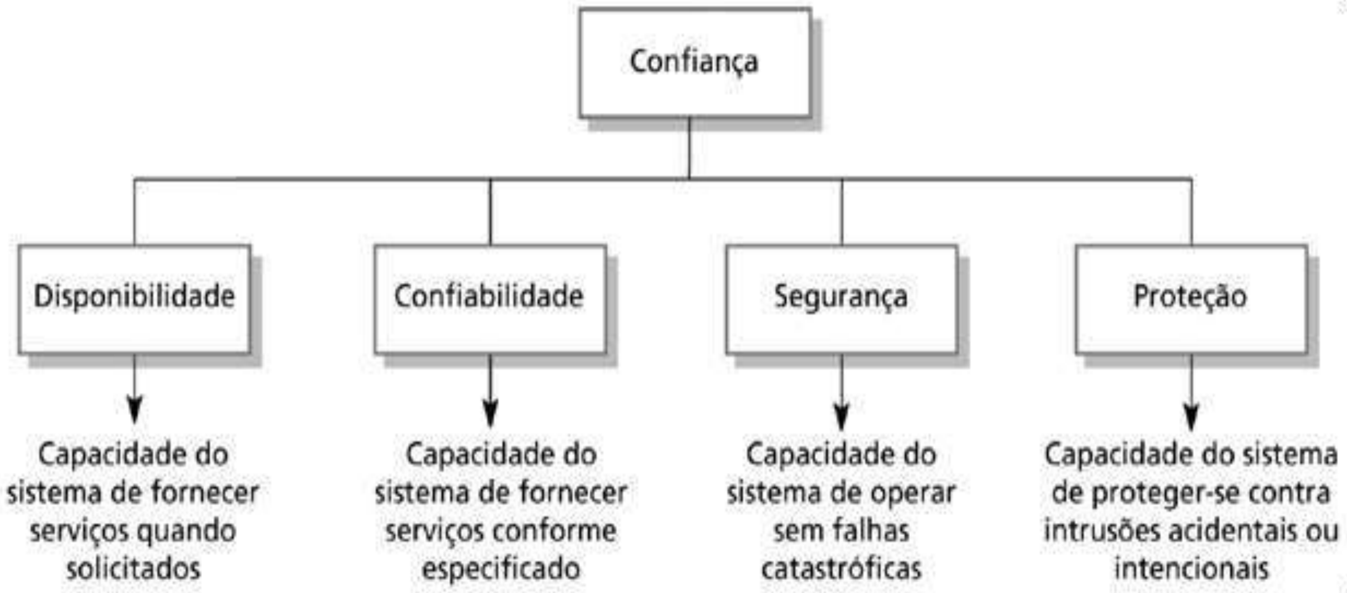
- O sistema deverá estar disponível para liberar insulina quando requisitado.
- O sistema apresentará confiabilidade e liberará a quantidade correta de insulina para neutralizar o nível corrente de açúcar no sangue.
- O requisito essencial de segurança é que doses excessivas de insulina nunca devem ser liberadas, já que isso é, potencialmente, uma ameaça de vida.

Confiança

- A confiança em um sistema equivale ao seu merecimento de confiança.
- Um sistema confiável é aquele em que os usuários depositam sua confiança.

Figura 3.3

Dimensões de confiança



Confiança

Disponibilidade — Capacidade do sistema de fornecer serviços quando solicitados

Confiabilidade — Capacidade do sistema de fornecer serviços conforme especificado

Segurança — Capacidade do sistema de operar sem falhas catastróficas

Proteção — Capacidade do sistema de proteger-se contra intrusões acidentais ou intencionais

Dúvidas?