Computers and Nuclear Energy - Fall 2013

- **EECE 499-01 Sp. Topic: Computers and Nuclear Energy**
  - CRN 85142
  - 3 credit hours
  - R1410 – 1700
  - LKD 3113
- **3rd offering – numbered?**
- **Instructor**
  - Dr. Charles Kim
  - (202)806-4821
  - ckim@howard.edu
  - Office Hours (LKD3014)
    - T 2:00 – 4:00 pm
    - W 4:00 – 5:00 pm
    - F - appointment
- **Web ---Syllabus, Notes, etc**
  - www.mwftr.com/CNE.html
- The class WAS sponsored by the grant from Nuclear Regulatory Commission: Grant #27-10-1123
- The class WAS team-taught by 2 professors and NRC guest speakers

Background

- Computers everywhere
- Computer Control Systems are replacing analog and electromechanical system – “Fly-by-Wire” → Invites a new set of problems
- Computer Related accidents, failures, and mishaps
- Car recalls
- Aircraft, cars, rocket launches, air line baggage handling systems, space systems, satellite launch, nuclear medicine, etc.
- Even in nuclear industry

Honda recalling 2.26M vehicles world-wide over automatic transmission failure

Posted by Vincent Van On August - 5 - 2011

- An F-14 drove off the deck of an aircraft carrier on command from its computer-controlled throttle.

What you see = What you have (behind the control room)?

- TMI (March 28, 1979)
  - Valve Indicator System
    - After the pressure-relief operation, the valve became stuck in the open position
    - Although the actuation voltage had been turned off and lights in the control room indicated that the valve was closed; it was actually stuck open.
    - Operators believed that the valve was closed, and coolant leaked from the vessel for almost 2 hours

Why Computers and Why Nuclear Energy

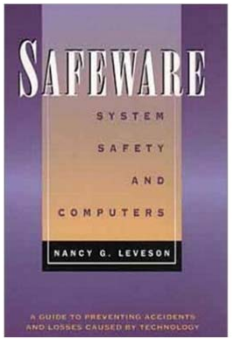
- Why do we focus on Computers
  - Ubiquitous computing
  - Embedded/Mobile/Intelligent Computing
  - Computer/Digital System Control
  - Are computers reliable?
    - Computer glitches in air line industry
    - Explosion of rockets due to coding error
- Safety-Critical System
  - Safety is the highest priority
  - A failure or accident causes substantial amount of damage
  - Failures are rare but with high impact– “Black Swan”
  - Computer controlled
  - Example: Nuclear power system, aircraft control system, petrochemical plant, oil exploration, nuclear weapon system, etc
  - We choose Nuclear Energy as the backdrop/background of safety-critical systems

Course Objectives & Topics

- Objectives
  - Understanding of general nuclear science and engineering concepts
  - Defense-in-Depth of computer system
  - Cyber-Security in Computerized Control Systems
- Topics of the Course
  - Nuclear System Fundamentals & Nuclear Power System Safety
  - Computer (H/W and S/W) reliability problems in mission critical systems
  - Investigation of Accidents caused by H/W or S/W
  - Defense-in-Depth of Computer Systems for System Safety

Course Material, expectation, and grading

- Textbook
  - None
- Related book - reference
  - “Safeware – System Safety and Computers” by Nancy Leveson
  - published by Addison-Wesley
  - ISBN: 0-201-11972-2
  - *NOTE: Used book is


SAFEWARE
SYSTEM SAFETY AND COMPUTERS
NANCY G. LEVESON
A GUIDE TO PREVENTING ACCIDENTS AND LOSSES CAUSED BY TECHNOLOGY

- Other Resources
  - Handouts
  - Book excepts
  - Articles
  - Reports
- Expectation
  - Attendance
  - Active Participation/Presentation
  - Reading Assignments
  - Writing Essay or Report
  - Everything counts
  - Professional manner

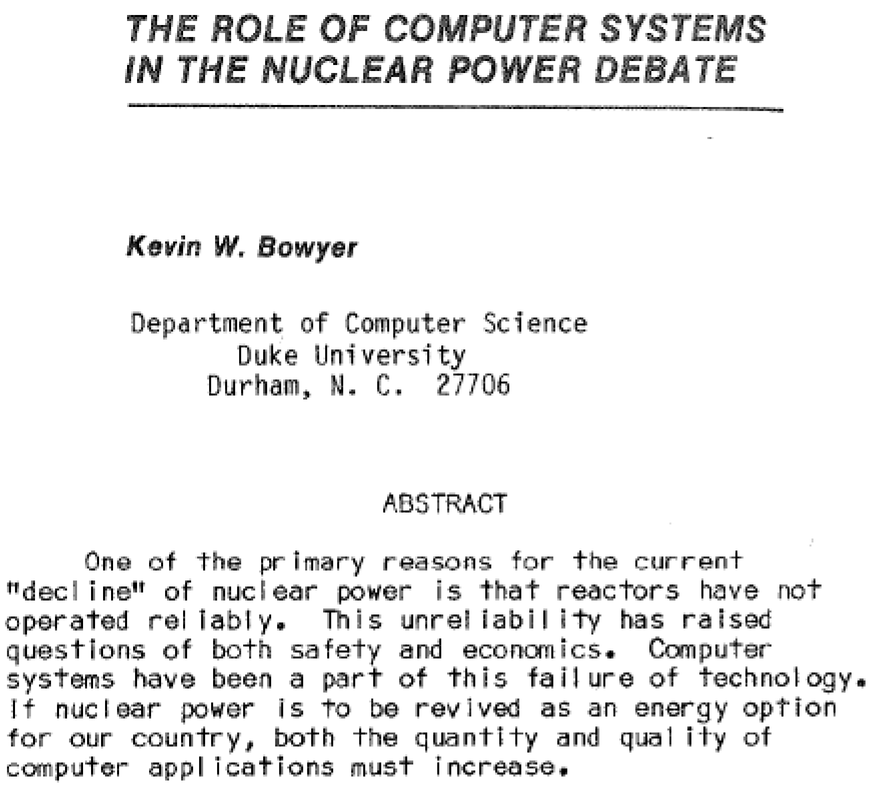
- Grading
  - Attendance (10%): only on-time arrival counts
  - Presentations (20%)
  - Assignments (65%):
    - Reading
    - Essay writing
    - Fact Reporting
    - Etc
  - Survey Participation (5%)
- Grades
  - A: 90 – 100
  - B: 80 – 89
  - C: 70 – 79
  - D: 60 – 69
  - F: 0 - 59

Class Structure

- 1. Lecturer
  - Computer-caused/related accident investigation
    - H/W and/or S/W
  - Defense-in-Depth Concept
  - Hardware Diversity
  - Software Reliability
  - Cyber-Security in computer control systems
- 2. Guest speakers
  - Subjects (Tentative)
    - **Nuclear Physics**
    - Reactors
    - Digital Instrumentation and Control
    - Security of Nuclear Power Plant
    - Cyber security
    - Licensing Process
    - Fukushima
- 3. On-line Study on Nuclear Physics

A long history of "Computers and Nuclear Energy"

- Computers & Society, 1980 (?)



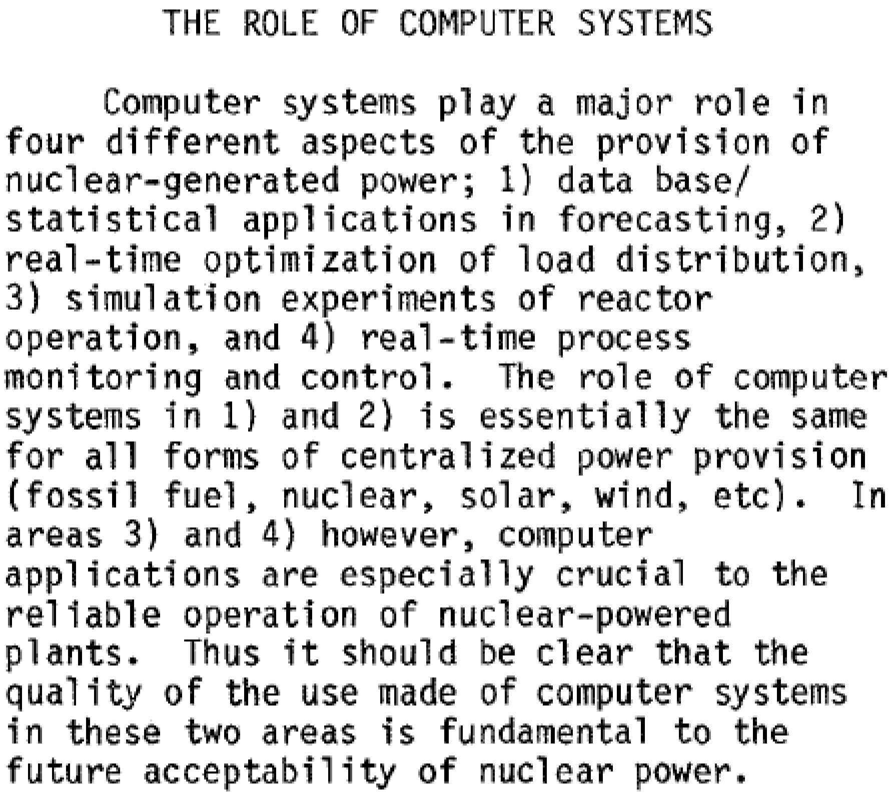
THE ROLE OF COMPUTER SYSTEMS IN THE NUCLEAR POWER DEBATE

Kevin W. Bowyer

Department of Computer Science
Duke University
Durham, N. C. 27706

ABSTRACT

One of the primary reasons for the current "decline" of nuclear power is that reactors have not operated reliably. This unreliability has raised questions of both safety and economics. Computer systems have been a part of this failure of technology. If nuclear power is to be revived as an energy option for our country, both the quantity and quality of computer applications must increase.



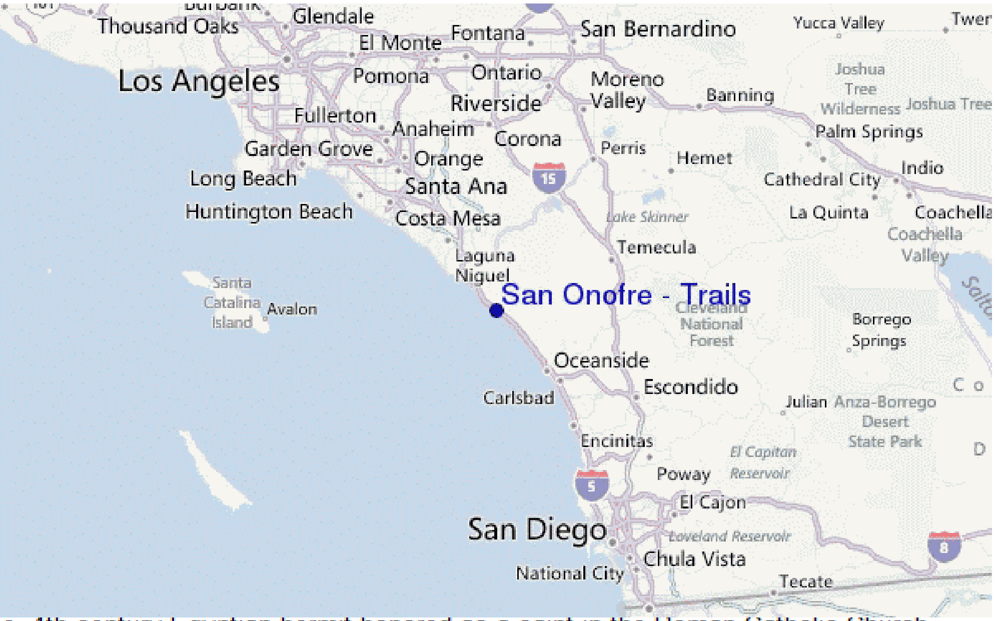
THE ROLE OF COMPUTER SYSTEMS

Computer systems play a major role in four different aspects of the provision of nuclear-generated power; 1) data base/statistical applications in forecasting, 2) real-time optimization of load distribution, 3) simulation experiments of reactor operation, and 4) real-time process monitoring and control. The role of computer systems in 1) and 2) is essentially the same for all forms of centralized power provision (fossil fuel, nuclear, solar, wind, etc). In areas 3) and 4) however, computer applications are especially crucial to the reliable operation of nuclear-powered plants. Thus it should be clear that the quality of the use made of computer systems in these two areas is fundamental to the future acceptability of nuclear power.

- **Role of Computers in Nuclear Energy**
  - Simulation Experiments of Reactor Operation
  - Real-time process monitoring and control

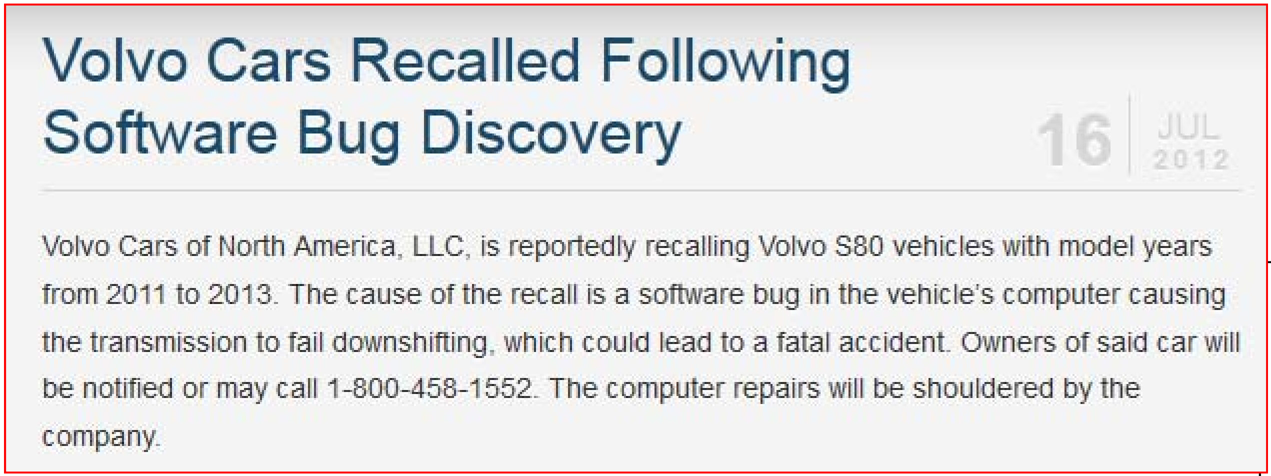
Computers in Nuclear Energy

- SONGS in 2012 (San Onofre Nuclear Generation Station) – Steam Pipe issues
  - Replacement steam generators that Edison installed in 2010 and 2011 proved to be defective, leading to a complete shutdown in January 2012
- Update: SCE decided to shut down San Onofre- summer 2013
  - $680 mission –defective steam generator
  - $2 billion - through 2017 (decommission)



San Onofre in Spanish and ***Sao Onofre*** in Portuguese, 4th-century Egyptian hermit honored as a saint in the Roman Catholic Church

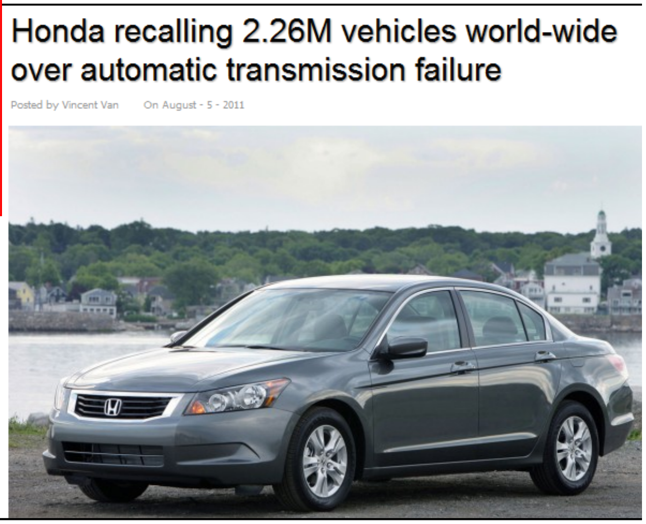
Recalls



Volvo Cars Recalled Following Software Bug Discovery

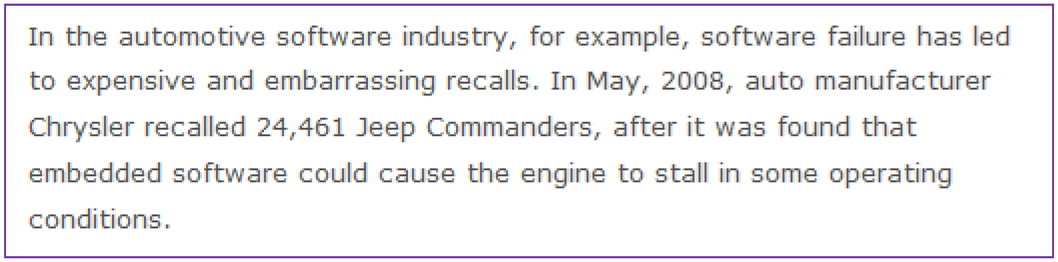
16 JUL 2012

Volvo Cars of North America, LLC, is reportedly recalling Volvo S80 vehicles with model years from 2011 to 2013. The cause of the recall is a software bug in the vehicle's computer causing the transmission to fail downshifting, which could lead to a fatal accident. Owners of said car will be notified or may call 1-800-458-1552. The computer repairs will be shouldered by the company.

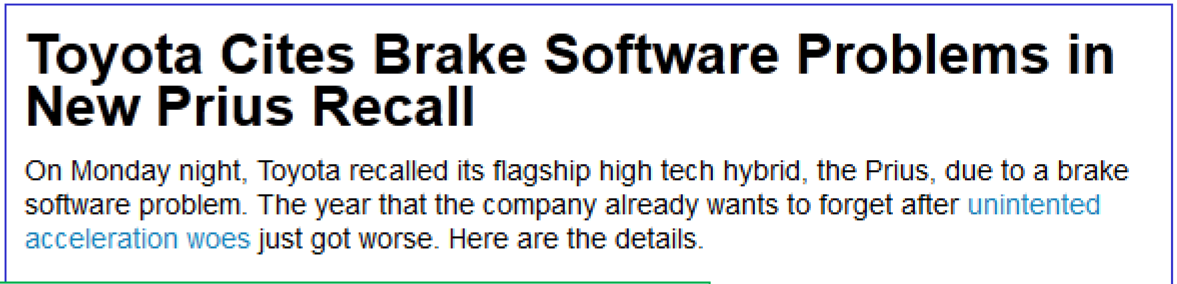


Honda recalling 2.26M vehicles world-wide over automatic transmission failure

Posted by Vincent Van On August - 5 - 2011

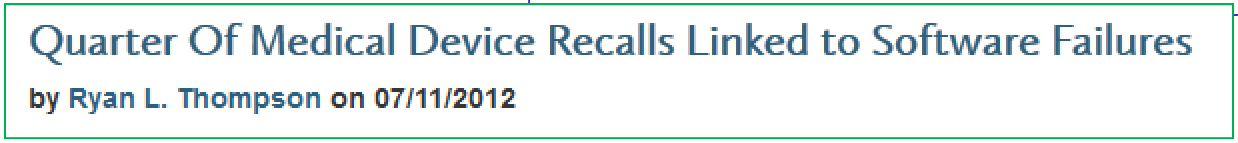


In the automotive software industry, for example, software failure has led to expensive and embarrassing recalls. In May, 2008, auto manufacturer Chrysler recalled 24,461 Jeep Commanders, after it was found that embedded software could cause the engine to stall in some operating conditions.



Toyota Cites Brake Software Problems in New Prius Recall

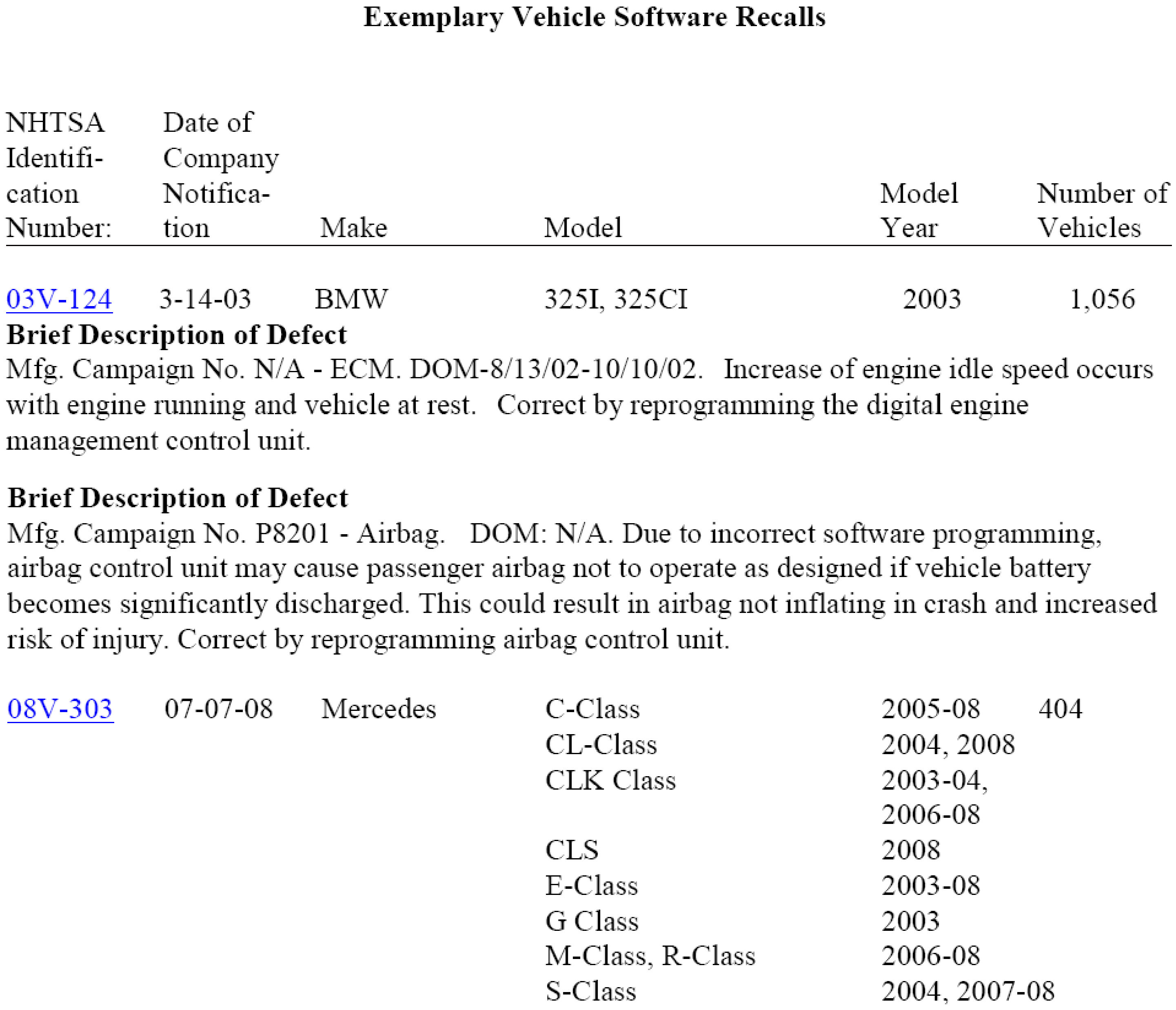
On Monday night, Toyota recalled its flagship high tech hybrid, the Prius, due to a brake software problem. The year that the company already wants to forget after unintented acceleration woes just got worse. Here are the details.



Quarter Of Medical Device Recalls Linked to Software Failures

by Ryan L. Thompson on 07/11/2012

Recall Details - Example



Exemplary Vehicle Software Recalls

NHTSA Identification Number:	Date of Company Notification	Make	Model	Model Year	Number of Vehicles
03V-124	3-14-03	BMW	325I, 325CI	2003	1,056

Brief Description of Defect

Mfg. Campaign No. N/A - ECM. DOM-8/13/02-10/10/02. Increase of engine idle speed occurs with engine running and vehicle at rest. Correct by reprogramming the digital engine management control unit.

Brief Description of Defect

Mfg. Campaign No. P8201 - Airbag. DOM: N/A. Due to incorrect software programming, airbag control unit may cause passenger airbag not to operate as designed if vehicle battery becomes significantly discharged. This could result in airbag not inflating in crash and increased risk of injury. Correct by reprogramming airbag control unit.

08V-303	07-07-08	Mercedes	C-Class	2005-08	404
			CL-Class	2004, 2008	
			CLK Class	2003-04, 2006-08	
			CLS	2008	
			E-Class	2003-08	
			G Class	2003	
			M-Class, R-Class	2006-08	
			S-Class	2004, 2007-08	

Summary

- Computers are used in controlling safety-critical systems
- H/W failures and S/W glitches
  - Rare but big impact
- Understanding how/why computer control system fails, and finding ways to prevent and mitigate computer failures
  - Difficult
  - Involves multi-disciplinary approach