

“Computers and Safety Critical Systems” [“CSCS → CS²”]

for

EECE 499 Sp Tp: Computers and Nuclear Energy
EECE 693 Sp Tp: Computers and Safety Critical Systems

Instructor: Dr. Charles Kim

Electrical and Computer Engineering
Howard University

Fall 2014

CS²– Fall 2014

- **Class**

- TR1410 – 1530
- LKD 3113

- **Instructor**

- Dr. Charles Kim
- (202)806-4821
- ckim@howard.edu
- Office Hours (LKD3014)
 - TWR 1030 - 1200

- **Web ---Syllabus, Notes, etc**

- www.mwftr.com/CS2.html [Under construction]

- The class WAS sponsored by the grant from Nuclear Regulatory Commission: Grant #27-10-1123

- The class had been team-taught by HU professors and NRC guest speakers

- Dr, Charles Kim – Safety Critical Embedded Systems
- Dr. Peter Keiller --- Software Reliability
- Dr. Emmanul Glakpe --- Neutron Physics
- NRC Researchers --- Reactors and Simulation

- Expectation for

- GR

- Presentation/Lecture
- Project
- Mathematical Risk Analysis

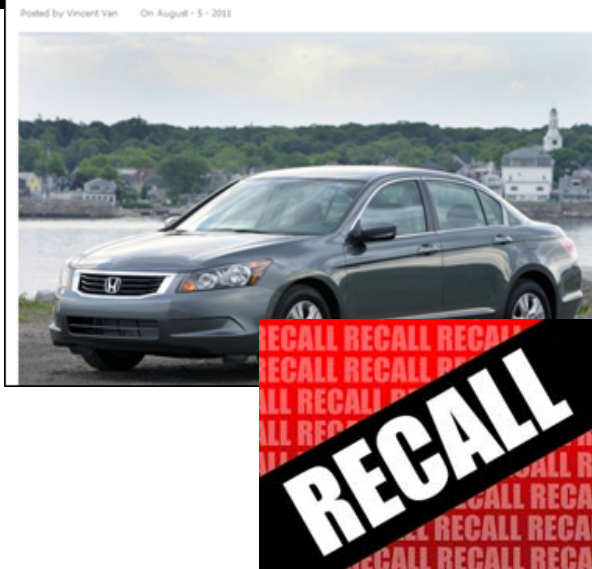
- UG

- Presentation
- Essay

Background

- Computers everywhere
- Computer Control Systems are replacing analog and electromechanical system – “Fly-by-Wire” → Invites a new set of problems “Computers are not intelligent enough to replace human operators”
- But people rely too much on computer control → Asian Airline crash landing in SFO
- Computer Related accidents, failures, and mishaps
- Car recalls
- Aircraft, cars, rocket launches, air line baggage handling systems, space systems, satellite launch, nuclear medicine, etc.

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



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

Toyota Camry/Prius Case

- Unintended Acceleration

**CLAIMS
JOURNAL**

View this article online: <http://www.claimsjournal.com/news/west/2013/10/09/238151.htm>

Toyota Acceleration Defect Caused Deaths and Injury, Lawyer Says

Toyota Economic Loss Settlement Administrator
c/o Gilardi & Co. LLC
P.O. Box 8090
San Rafael, CA 94912-8090
March 14, 2014

Re: Toyota Motor Corp. Unintended Acceleration Marketing,
Sales Practices, and Products Liability Litigation
Claim Number: TMUA1-27067168-4-C

Check Number: 1096321
Check Amount: \$125.00

- RECALL for possible a sudden stall

latimes.com

Toyota recalls 1.9 million Prius hybrids to fix software problem

By Jerry Hirsch

The Prius recall includes 1.9 million vehicles sold from 2010 through 2014 model years.

Toyota said it will update software in the electronic controls of the car.

The software's current settings could create heat in some of the transistors in the circuits of the car, damaging the parts. When this happens, warning lights on the dashboard activate. In rare circumstances, the hybrid system might shut down while the vehicle is being driven, creating a sudden stall.

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

Scope of the class

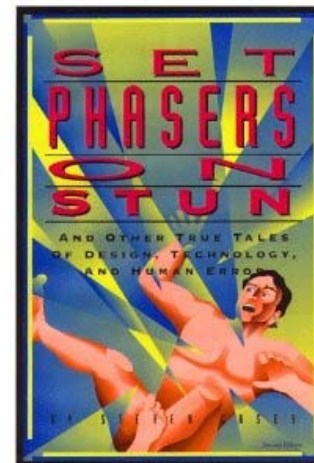
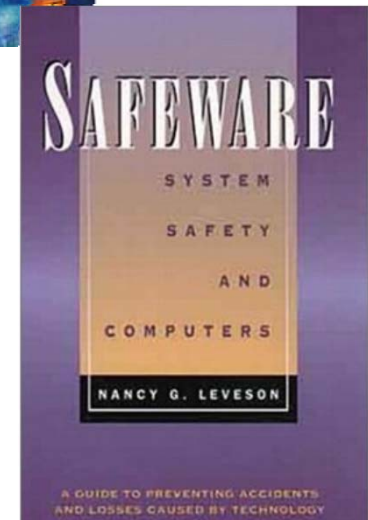
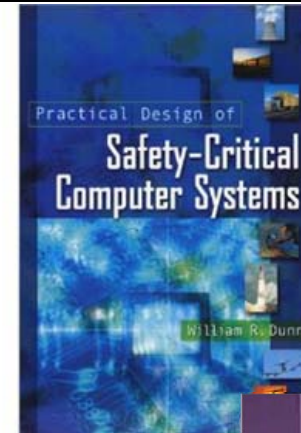
- Why do we focus on Computers
 - Ubiquitous computing
 - Embedded/Mobile/Intelligent Computing
 - Computer/Digital System Control
 - Are computers reliable?
 - Computer glitches in airline industry --- random/design hardware failure
 - Explosion of rockets due to coding error --- Software/Coding failure
- 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, automobile engine control, airbag, anti-lock breaking, etc.

Course Objectives & Topics

- Objectives
 - Understanding of general system safety concepts
 - Defense-in-Depth of computer system
 - Software Reliability
 - 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 safety-critical systems
 - Investigation of Accidents caused by H/W or S/W
 - Defense-in-Depth of Computer Systems for System Safety
 - Safety-Critical Computer System Design
 - Cybersecurity in Safety-Critical Computer Systems

Course Material

- Textbook
 - “Practical Design of Safety-Critical Computer Systems: by William R. Dunn
 - Reliability Press
 - ISBN 0-9717527-0-2
- Related book - reference
 - “Safeware – System Safety and Computers” by Nancy Leveson
 - published by Addison-Wesley
 - ISBN: 0-201-11972-2
 - *NOTE: Used book is cheap
- Related Book – Reference 2
 - “Set Phasers on Stun” by Steven Casey
- Other Resources
 - Handouts
 - Book excerpts
 - Articles
 - Reports



Assignments + Grading

- Grading
 - Attendance (10%): only on-time arrival counts
 - Presentations (20%)
 - Assignments (40%):
 - Reading material summarization
 - Essay writing
 - Project + Reporting
 - Final Exam (30%)
 - Comprehensive
 - Descriptive
- Grades
 - A: 90 – 100
 - B: 80 – 89
 - C: 70 – 79
 - D: 60 – 69
 - F: 0 - 59

Class Structure

- 1. Lecture
 - Computer-caused/related accident investigation
 - H/W and/or S/W
 - Safety-Critical Compute System Design and Evaluation
 - Defense-in-Depth and Diversity (D3) Concept
 - Software Reliability --- [Dr. Peter Keiller](#)
 - Cyber-Security in computer control systems
- 2. Guest speakers
 - Subjects (Tentative)
 - **Nuclear Physics** --- [Dr. Emmanuel Glakpe](#)
 - Reactors
 - Security of Nuclear Power Plant
 - Cyber security
 - 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.

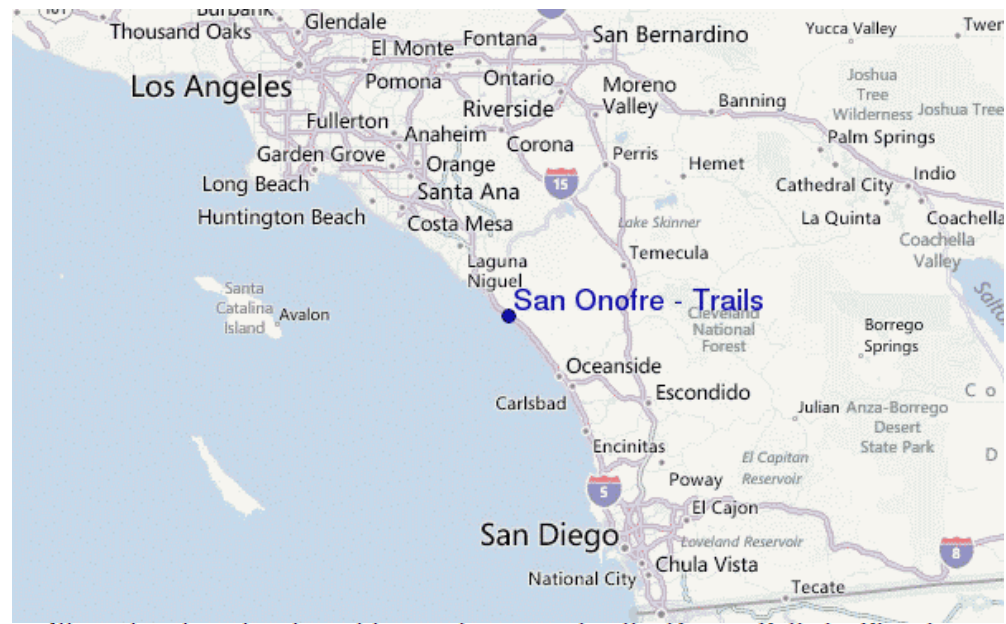
THE ROLE OF COMPUTER SYSTEMS

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

Mechanical Problems from Simulation Error ?

- 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 million –defective steam generator
 - \$2 billion - through 2017 (decommission)



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

Fault in Nuclear Software

Hitachi Finds Nuclear Software Fault; Undetected for 28 Years

By Shigeru Sato - April 10, 2008 22:57 EDT

April 11 (Bloomberg) -- [Hitachi Ltd.](#), Japan's third-largest builder of nuclear reactors, discovered a programming error in software used for almost three decades to measure the impact of earthquakes on pipes at atomic power stations.

The mistake, made by a Hitachi programmer, allows the software to underestimate the quake impact on steel pipes associated with eight nuclear reactors owned by six utilities, including [Tokyo Electric Power Co.](#), Hitachi spokesman [Keisaku Shibatani](#) said by telephone.

Confidence in the safety of Japan's nuclear power plants has been shaken after a 6.8-magnitude earthquake caused a fire and radiation leaks at a Tokyo Electric facility in Niigata prefecture last July. Twelve power producers, responding to a government request, revealed in March 2007 more than 300 cases of improper safety practices. Hitachi reported the software problem to the utilities this week, Shibatani said.

"It was a human error," he said. "We're closely looking into this now."

Fukushima 1 Year Earlier

Computer problems hit three nuclear plants in Japan

January 03, 2000

by Martyn Williams

Tokyo IDG Only a handful of computer problems have been reported in Japan in the new year to date; however, at least three hit systems associated with nuclear power plants, according to the government and power generating companies.

The potentially most serious problem occurred not at midnight but at 858 a.m. local time on Jan. 1 at the Fukushima Number 2 nuclear power plant of Tokyo Electric Power Co. TEPCO. The system that shows the position of the control rods in the reactor core failed, leaving operators unable to gauge the rods positions using the system.

TEPCO officials said a plant processing computer enabled operators verify the position of the rods until the problem was located. Engineers confirmed the power supply and central processor associated with the system were fine and, at 1115 a.m., found the problem to be in a clock used in the board that controls the display screen. The clock was set to Feb. 6, 2036. After being reset to Jan. 1, 2000, the system returned to normal operation at 212 p.m., TEPCO officials said.

The cause of the failure is still under investigation.

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 unintended 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 Identifi- cation Number: | Date of Company Notifica- tion | 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 | |

Missile Launch Control Glitch

Computer problem blamed for missile site malfunction

October 27, 2010 | By Larry Shaughnessy, CNN Pentagon Producer

A malfunctioning launch control center for a portion of the nation's nuclear missiles remained offline Wednesday as investigations continued into a weekend computer problem that disrupted communications with more than 10 percent of America's land-based nuclear missiles.

Early indications are that Saturday's disruption to one of the launch control centers linked to Warren Air Force Base in Wyoming lasted longer than an hour, Lt. Col. John Thomas said. The problem appears to be very similar to glitches at two other nuclear missile sites in the late 1990s.

Share

Twitter

Email

Recommend

114 recommendations. [Sign Up](#) to see what your friends recommend.



An Air Force technician inspects a Minuteman III missile in a silo in North Dakota.

AFP/GETTY IMAGES

Costa Concordia

- Accident: 1/13/2012
- Ship weighs more than 100 tons
- Measures 951ft. In length
- Maximum Speed is 23mph
- About 4,200 people were on the ship
- First trip July 14, 2006
- Estimated Cost of Ship \$350 million
- 17 Decks
- Larger than Titanic
- Largest ship ever for Carnival
- Sophisticated automatic tracking system
- Paper and Electronic Charts with Radar Overlay

Costa Concordia - Accident

- what the captain said:
 - Captain Schettino stated that the rock he hit was not on his map for routing
 - Italian Coast Guard showed evidence that the rock was very well charted
 - The reason he fled the ship was because he accidentally fell into a safety boat
- Computer or Human Error? Or Both?
 - According to the reports and investigation this was considered a **human error** due to the fact the captain made a maneuver with the ship that was not authorized.
 - Following contact, the **ship suffered a blackout**. Emergency electrical power would be expected to have kicked in. Propulsion and steering were lost or minimized, thereby adversely affecting an initial attempt to bring the ship closer to the port beyond the rock for assistance

Accident and Complication of the Cause Determination: Example – “Friendly Fire”

- April 14, 1994
- Iraq
- No Fly Zone
- AWACS (Airborne Warning and Control System)
- F-15 fighters
- UH-60 Helicopters (“Black Hawk”)
- 26 Peacekeepers killed
- Many approaches to understand the incident
 - Social and organizational approach
 - My view: component intermittency of IFF (Identification Friend or Foe)

Stuxnet at Natanz



Smart Grid and Smart Meter Cyber Vulnerability

Four Ways to Hack the Smart Grid

By [Preston Gralla](#)

Published September 01, 2009

Tags: [Data Centers](#), [Servers](#), [More...](#)

Attack Smart Meter RAM

Hack the Meter's Digital radio

Hack the Meter Wirelessly

Spread Malware Throughout the Network

- Smart Meter Hack?

Electricity Theft with Smart Meter Tampering

- Theft with Smart Meter in Malta

malta INDEPENDENT

malta INDEPENDENT



Sparks over smart meter theft scandal

02/22/2014

<http://www.independent.com.mt/uploads/media/NewspaperArticle-MainImage/ArticlesExtraLarge/3968892934->

Sparks and calls for political responsibility are flying fast and furious over the smart meter electricity racket scandal made public by the government earlier this week, with both the government and Opposition calling on each other to assume political responsibility for the scam which, according to the government, accounted for some 10 per cent of all the electricity generated by Enemalta in 2012 – costing the taxpayer some €30 million in that year alone.

According to reports, those running the racket had charged €1,200 per residential smart meter, with charges for tampering with smart meters in commercial establishments much higher.

Dr Mizzi had said that the scam had amounted to some 10 per cent of the total generation of electricity by Enemalta, costing taxpayers around €30 million in 2012 alone.

How about this case close to home



DC Police Department @DCPoliceDept · 3h

Traffic congestion due to signal malfunctioning:

*14th St & New York Ave NW - DDOT notified.

//7066



- Signal Timing Problem caused Traffic Jam

1/2 Update:

TCO'S are placed along 14th St to help ease the congestions. A work order has been submitted to check signal operation

Charles Kim – Hov

Software Blues

Hidden Bugs

- OpenSSL Project: (Secure Sockets Layer) + (Transport Layer Security)

Date

Newsflash

06-Aug-2014: **Security Advisory:** nine security fixes

06-Aug-2014: OpenSSL 1.0.1i is now **availabl**

06-Aug-2014: OpenSSL 1.0.0n is now **availab**

06-Aug-2014: OpenSSL 0.9.8zb is now **availa**
fixes

22-Jul-2014: Beta 2 of OpenSSL 1.0.2 is now

Heartbleed Bug: What is it, Who is handling our security

Heartbleed Bug has raised eyebrows of all the users across the globe and security advocates and surprisingly, only a few people are handling our internet security.

g+ Share 2 f Like 58 t Tweet 23 in Share 8 + reddit this!

New 'Heartbleed' bug poses major threat to user data

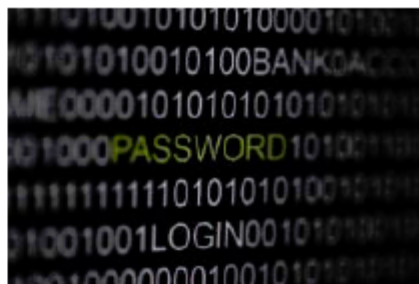
5:35am EDT

BOSTON (Reuters) - A newly discovered bug in widely used Web encryption technology has made data on many of the world's major websites vulnerable to theft by hackers in what experts say is one of the most serious security flaws uncovered in recent years.

The finding of the so-called "Heartbleed" vulnerability, by researchers with Google Inc and a small security firm Codenomicon, prompted the U.S. government's Department of Homeland Security to advise businesses on Tuesday to review their servers to see if they were using vulnerable versions a type of software known as OpenSSL.

It said updates are already available to address the vulnerability in OpenSSL, which could enable remote attackers to access sensitive data including passwords and secret keys that can decode traffic as it travels across the Internet.

"We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace," Codenomicon said on a website it built to provide information about the threat, heartbleed.com.



How errors are inserted

Heartbleed: Is it a simple Programming Error?

What is Heartbleed? Heartbleed is a bug discovered by Codenomicon employees Riku, Antti, and Matti, as well as Google employee Neel Mehta this week. Heartbleed is essentially a programming error that leaves all forms of Internet data open to hackers. It was introduced into the OpenSSL software library by 31-year-old Robin Seggelmann, a Frankfurt, Germany developer who says that it was likely introduced while he was working on OpenSSL bug fixes around two years ago. "I was working on improving OpenSSL and submitted numerous bug fixes and added new features. In one of the new features, unfortunately, I missed validating a variable containing a length." The error was also missed by a reviewer responsible for double-checking the code, "so the error made its way from the development branch into the released version." Seggelmann said.

It's interesting to think about how a line of code could open a world of crime and identity theft for millions, but it's true. Sometimes the smallest items in the world can do a lot of damage.

Seggelmann denies that he introduced the programming error intentionally, and his testimony is credible. Why would he introduce a massive programming error while optimizing OpenSSL software against bug fixes at the same time?

While the Heartbleed bug seems focused on user data and hackers, it's also possible that the server could extract personal user data from any client. In other words, with the greater exchange of data between clients, servers, and normal users, data extraction is possible from any of these three mediums. A malicious server can do as much damage as a hacker if the Heartbleed bug is left unchecked. Even if someone patches up the Heartbleed vulnerability at a given site, one can still experience a reverse Heartbleed vulnerability and still be subject to a data encryption attack.

New Challenges of Widespread use of Computers

- Computers everywhere
- Computer-Caused accidents and failures
- Methods of **safe computer control** system is **lagged** behind the development of such systems
- **Safety engineering** does **not include computers** (software in particular)
- Software reliability (or safety) is **not easy** to adopt in to the existing reliability program
- Computer engineers (software) are **not prepared** to cope with safety problems
- **Communication problems** among system engineers, IT specialists, software engineers, operators, programmers, etc.
- And, Human Errors.
- Further, Systems that cause human errors.
- Human/Malware attackers



Summary

- Assignment#1:
 - Read the 2 articles and summarize their points and discuss them with respect to compute system failures.
 - 2 – 3page length report: due on 09/11/2014
- 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