# SFWR ENG 3K04
# Software Development

Alan Wassyng

September - December 2019

Many of these slides were provided by the authors of "Fundamentals of Software Engineering", 2nd edition - Ghezzi, Jazayeri & Mandrioli. Some have been edited.

## Course Info

- Web-site:
  http://avenue.mcmaster.ca/
- Recommended Reference:
  *"Fundamentals of Software Engineering" Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli, Second Edition.*
- 2 Assignments = 1 Project - 35%*
- Mid Term Exam - 25%* Both exams are multiple-
- Final Exam - 40%* choice & open book
- Bonus marks of 1%, 2% or 3% are available by participating in competitions such as the McMaster Engineering Competition (MEC2019)*

* Effective if average grade on final & mid term exams is ≥ 50%
If average of final & mid term exams < 50% then the final grade for the course is that average.

1

## TAs

To be confirmed

2

## Calendar Description

- Software design process
- Professional responsibility
- Using specifications
- Documentation
- Module interface specification
- Module internal documentation
- Coding styles
- Portability
- Software inspection
- Software testing

3

# Calendar Description

- Software design process
- Professional responsibility
- Using specifications
- Documentation
- Module interface specification
- Module internal documentation
- Coding styles
- Portability
- Software inspection
- Software testing

What we will concentrate on:

| |
|---|
| Embedded software |
| Development Life-Cycle |
| Traditional & Model-Driven |
| Requirements |
| Design |
| Implementation |
| Validation & Verification |
| Dependability & Safety |

4

# Important Explanation

Methods & long term knowledge

| Lectures | Project |
|---|---|
| Introduction to SE | |
| Motivation | Form groups |
| Why is software difficult? | Matlab/Simulink/Stateflow |
| Requirements | |
| Formal notations | Understand requirements |
| Hazard/threat analysis | |
| Design principles & documentation | |
| Traditional | Assignment 1 |
| Model driven | |
| Verification (testing) | |
| More formal approaches | Assignment 2 |
| Pre-post conditions | |
| Validation | |

Application of methods & knowledge to build skills

5

# My Background

- Applied Math/Scientific Computation – till 1982
  - U Witwatersrand 1968-72 (student), 1973-79 faculty
  - U Minnesota 1979-82 faculty (Civil & Mineral Eng)
  - A*x*=*b* (large systems, applications in Rock Mechanics)
- Use of PCs in Engineering Education – 1982-1986
  - U Minnesota faculty (Civil & Mineral Eng), IBM funded project
- Computer Consulting – 1987-(2002)
  - General computer consulting
  - Safety critical software for the nuclear industry
    - Methodology for OPG safety-critical software
    - Darlington Nuclear Generating Station – Shutdown System(s)
- McMaster U – 2002-
  - Department of Computing and Software
  - McMaster Centre for Software Certification (McSCert) – Co-founder & Director 2009-2017
  - Software Certification Consortium (SCC) Co-founder, Chair

6

# Current Research

- Software Certification (Large funded projects)
  - Medical devices – Federal Drug Administration
  - Nuclear Power – OPG, Candu Energy, SWI, Nuclear Regulatory Commission
  - Financial Legacy Systems – LSI
  - eHealth
- Automotive Software
  - Safety & Model Management with GM – 2017-2020
  - Project on Certification with Toyota ITC , US – 2015-2018
  - Software development for FCA as part of the LEAP/LEAP2 projects – 2013-…
  - IBM SOSCIP Project on Safe Insulin Pumps – 2012-2014
  - Model Driven Engineering for Automotive Software – APC project with GM and IBM/GM – project called “NECSIS”, ended 2016
  - IBM Shared University Research Award – multi-core processors to develop safer cars in a “smarter transportation” project – 2010
- Safety-Critical Software
  - Timing issues in hard real-time systems
  - Requirements
  - Assurance Cases, Integrated methods/tools & model driven development

7

# Software Certification Consortium

- Co-founded SCC in 2007
- Serve as Chair of the Steering Committee
- Industry, government agencies & academia
- Mandate:
  - How do we build critical software-intensive systems so that they can be certified?
  - How do we certify those systems?
- https://cps-vo.org/group/scc
  - Click on Meetings to see previous meetings including presentations from many of them
  - Held our 20th meeting this past May

8

# Software Engineering - 1

- The application of engineering to software
- Built on mathematics & computer science dealing with software systems
  - large and complex
  - built by teams
  - exist in many versions
  - active for many years
  - undergo changes

9

## Software Engineering - 2

- Application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software (IEEE 1990)
- Multi-person construction of multi-version software (Rendall 1978, remark to David Parnas)

10

## SE in system design

- SE part of larger projects
- Embedded
  - Software requirements to be balanced against others
    - e.g., telephone switching systems
      - certain requirements can only be met by hardware, software, and special devices
  - Software constrained to work in a very specific environment
  - Need disciplined software development
  - Cyber Physical Systems (CPS) have become very complex and require a very well-trained work force

11

# Recent software failures

- The following are examples from news services in the past few years

12

# Health-care database

## 2,000 lab results mixed-up in Calgary

By SCOTT DEVEAU
Monday, July 11, 2005 | Updated at 5:14 PM EDT
Globe and Mail Update

A computer glitch has mixed up 2,000 lab results taken during the past two months in the Calgary region, officials said Monday.

The Calgary Health Region has been scrambling to reach the 378 health-care providers that accessed its database since it underwent software upgrades in May. A glitch in the new program has mixed up 2,000 lab results, according to officials.

13

# Pacemaker recall

More Headlines from June 23, 2005

**IN THE WAKE OF DEFIBRILLATOR RECALL, CARDIOLOGISTS' GROUP TO PREPARE GUIDELINES FOR MANUFACTURERS TO FOLLOW WHEN PATTERN OF MALFUNCTIONS IS DISCOVERED**

Date Published: June 23, 2005
Source: Newsinferno.com News Staff

The sudden recall of almost 50,000 implanted defibrillators manufactured by Guidant Corp. on June 17 has many experts questioning a monitoring system which essentially leaves the matter of disclosure, with respect to potential flaws in such critical medical devices, entirely to the manufacturer.

In issuing the recall, Guidant stated the Ventak Prizm 2 DR should be monitored and will be replaced if necessary by Guidant at no charge. For the models with potential memory errors, Guidant is recommending an in office programming change that can reduce the risk until Guidant is able to design a software solution. The remaining devices should be monitored at three-month intervals and undergo a complete trouble-shooting procedure if a yellow warning screen appears on the programmer.

14

# Car stall due to software

**NEW YORK (CNN/Money) - A software problem is causing some Toyota Prius gas-electric hybrid cars to stall or shut down while driving at highway speeds, according to a published report.**

The *Wall Street Journal* reports that the problem involves Priuses from the 2004 model year and some early 2005 models.

The newspaper reports the National Highway Traffic Safety Administration has logged 13 reports of the engine shutdowns, while Edmunds.com, a popular vehicle-information and shopping site, has had 13 individuals post complaints in a Prius forum. Some of the cars that shut down had to be towed to the shop before they could be restarted.

The newspaper quotes an official from Toyota as saying the stalling problem is due to a software glitch in its sophisticated computer system.

15

# UK tax software

## EDS threatened with legal action over £51m tax fiasco

Andy McCue
silicon.com
June 22, 2005, 09:35 BST

The Inland Revenue is threatening to drag EDS through the courts unless compensation is agreed for overpayments that resulted from problems with the new tax credit IT system.

A software error on the EDS-designed tax credits IT system resulted in overpayments to 455,000 households in 2003 totalling almost £100m and the Inland Revenue has admitted it may be forced to write off more than £50m of that sum.

16

# Infusion pumps

## Baxter COLLEAGUE Infusion Pumps Malfunction Yet Again

**Oct 24, 2007 | Parker Waichman Alonso LLP**

Baxter COLLEAGUE infusion pumps have been malfunctioning again under certain conditions, prompting new warnings from the company. According to a letter sent to its Canadian customers, Baxter has received reports of incidents where the COLLEAGUE triple channel infusion pumps stopped infusing. According to the "Urgent Device Correction" notice issued by Baxter, the company is working on a software solution to fix the problem with its COLLEAGUE triple channel infusion pumps.

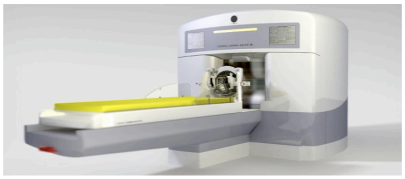
The Baxter infusion pumps affected by the correction notice include Baxter COLLEAGUE triple channel Mono, CX and CXE Volumetric infusion pumps with product codes of 2M8153, 2M8163, 2M9163, DNM8153 and DNM9183. According to the correction notice, Baxter has received reports from 3 Canadian customers of at least six instances where defective COLLEAGUE infusion pumps stopped infusing. In each instance, the pump issued an audible and visual alarm and displayed the error code 16:310:867:0002 before it stopped. Baxter said that this malfunction of the COLLEAGUE infusion pumps occurred when the capacity of the buffer memory device was exceeded. While no injuries have been reported in relation to the defective Baxter COLLEAGUE infusion pumps, the company said that lab tests of the pumps showed that this malfunction had a high probability of occurring under certain circumstances.

17

# Gamma Knife

## 'Known Software Bug' Disrupts Brain-Tumor Zapping

By Kevin Poulsen ✉ October 16, 2009 | 4:19 pm | Categories: Glitches and Bugs

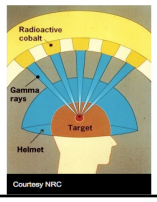


The maker of a life-saving radiation therapy device has patched a software bug that could cause the system's emergency stop button to fail to stop, following an incident at a Cleveland hospital in which medical staff had to physically pull a patient from the maw of the machine.

288 diggs digg it

The bug affected the Gamma Knife, a device resembling a CT scan machine that focuses radiation on a patient's brain tumor while leaving surrounding tissue untouched. A patient lies down on a motorized couch that glides into a chamber, where 201 emitters focus radiation on the treatment area from different angles. The patient wears a specialized helmet screwed onto his skull to ensure that his head doesn't move and expose the wrong part of the brain to the machine's pinpoint tumor-zapping beams.

Positioning is vital in the procedure, so when the couch moved out of position during a treatment at an university hospital in Cleveland last December, staffers hit the "emergency stop" button, expecting the couch to pull the patient out of the Gamma Knife, and the radiation shields at the mouth of the machine to automatically close. Instead, according to a report eventually filed with the Nuclear Regulatory Agency, nothing happened.




"Staff had to manually pull out the couch from the Gamma Knife and manually close the doors to the Gamma Knife to shield the source," reads the report, which states that neither the patient nor the workers were harmed. "Radiation exposure to all individuals involved with the incident was minimal."

When the hospital called the company that makes the Gamma Knife, it learned that there was a "known software bug problem" affecting the unit's couch sensors. Known, anyway, to the company, Stockholm-based Elekta AB.

18

# Therapy Planning

**November 2000 -- National Cancer Institute, Panama City.** In a series of accidents, therapy planning software created by Multidata Systems International, a U.S. firm, miscalculates the proper dosage of radiation for patients undergoing radiation therapy.

Multidata's software allows a radiation therapist to draw on a computer screen the placement of metal shields called "blocks" designed to protect healthy tissue from the radiation. But the software will only allow technicians to use four shielding blocks, and the Panamanian doctors wish to use five.

The doctors discover that they can trick the software by drawing all five blocks as a single large block with a hole in the middle. What the doctors don't realize is that the Multidata software gives different answers in this configuration depending on how the hole is drawn: draw it in one direction and the correct dose is calculated, draw in another direction and the software recommends twice the necessary exposure.

At least eight patients die, while another 20 receive overdoses likely to cause significant health problems. The physicians, who were legally required to double-check the computer's calculations by hand, are indicted for murder.

19

# Radiation Overdose

From the New York Times

## Radiation Offers New Cures, and Ways to Do Harm

By WALT BOGDANICH
Published: January 23, 2010

As Scott Jerome-Parks lay dying, he clung to this wish: that his fatal radiation overdose — which left him deaf, struggling to see, unable to swallow, burned, with his teeth falling out, with ulcers in his mouth and throat, nauseated, in severe pain and finally unable to breathe — be studied and talked about publicly so that others might not have to live his nightmare.

SIGN IN TO E-MAIL
PRINT
SINGLE PAGE
REPRINTS
SHARE



Enlarge This Image

For his last Christmas, Mr. Jerome-Parks rested his feet in buckets of sand his friends had sent from a childhood beach.

Sensing death was near, Mr. Jerome-Parks summoned his family for a final Christmas. His friends sent two buckets of sand from the beach where they had played as children so he could touch it, feel it and remember better days.

Mr. Jerome-Parks died several weeks later in 2007. He was 43.

A New York City hospital treating him for tongue cancer had failed to detect a computer error that directed a linear accelerator to blast his brain stem and neck with errant beams of radiation. Not once, but on three consecutive days.

20

# And Again

THE RADIATION BOOM

## A Pinpoint Beam Strays Invisibly, Harming Instead of Healing

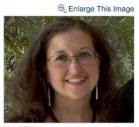
By WALT BOGDANICH and KRISTINA REBELO
Published: December 28, 2010

The initial accident report offered few details, except to say that an unidentified hospital had administered radiation overdoses to three patients during identical medical procedures.

RECOMMEND
TWITTER
COMMENTS (185)
SIGN IN TO E-MAIL
PRINT
SINGLE PAGE
REPRINTS
SHARE



Enlarge This Image



Marci Faber is nearly comatose after a treatment mistake.

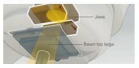
**The Radiation Boom**

*Missing the Target*

Articles in this series examine issues arising from the increasing use of medical radiation and the new technologies that deliver it.

Previous Articles in the Series »

**Multimedia**



It was not until many months later that the full import of what had happened in the hospital last year began to surface in urgent nationwide warnings, which advised doctors to be extra vigilant when using a particular device that delivers high-intensity, pinpoint radiation to vulnerable parts of the body.

Marci Faber was one of the three patients. She had gone to Evanston Hospital in Illinois seeking treatment for pain emanating from a nerve deep inside her head. Today, she is in a nursing home, nearly comatose, unable to speak, eat or walk, leaving her husband to care for their three young daughters.

Two other patients were overdosed before the hospital realized that the device, a linear accelerator, had inexplicably allowed radiation to spill outside a heavy metal cone attachment that was supposed to channel the beam to a specific spot in the brain. One month later, the same accident happened at another hospital.

…

In the last five years, SRS systems made by Varian and its frequent German partner, Brainlab, have figured in scores of errors and overdoses, The New York Times has found. Some mistakes were caused by operator error. In Missouri, for example, 76 patients were overradiated because a medical physicist did not realize that the smaller radiation beam used in radiosurgery had to be calibrated differently than the larger beam used for more traditional radiation therapy.

21

# Pacemaker Security

## FDA issues new security guidelines so that your pacemaker won't get hacked

Posted Dec 28, 2016 by Taylor Hatmaker (@tayhatmaker)

This week, the US Food and Drug Administration issued a set of recommendations for securing medical devices that could jeopardize the safety and privacy of their users. The report, titled "Postmarket Management of Cybersecurity in Medical Devices," focuses on security throughout the lifecycle of a device, emphasizing that robust cybersecurity is an ongoing process that requires maintenance and regular software updates, just like any non-medical piece of hardware would.

22

# Pacemaker Security

## FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

By Charlie Osborne for Zero Day | August 30, 2017 -- 10:31 GMT (03:31 PDT) | Topic: Security

File photo

In what may be a first, patients with heart conditions that are using particular pacemaker brands will have to visit their doctors for firmware updates to keep their embedded devices safe from tampering.

RELATED STORIES

Security
Android security: Multiple bootloader bugs found in major chipset vendors' code

Security
How blockchain technology can transform the security industry

Mobility
BT announces 'business platform as a service'

Innovation
Data61 and ANU establish research institute to tackle AI

NEWSLETTERS

SEE ALL

23

# Medical Device Security

## MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

THIERRY DOSOGNE/GETTY IMAGES

HACKED MEDICAL DEVICES make for scary headlines. Dick Cheney ordered changes to his pacemaker to better protect it from hackers. Johnson & Johnson warned customers about a security bug in one of its insulin pumps last fall. And St. Jude has spent months dealing with the fallout of vulnerabilities in some of the company's defibrillators, pacemakers, and other medical electronics. You'd think by now medical device companies would have learned something about security reform. Experts warn they haven't.

24

# Insulin Pump Security

## Johnson & Johnson warns of insulin pump hack risk

Elizabeth Weise, USATODAY Published 12:57 p.m. ET Oct. 4, 2016 | Updated 7:35 a.m. ET Oct. 5, 2016

Johnson & Johnson, a major maker of medical devices has for the first time issued a warning about a potential computer security flaw in a consumer product, but cautions that the danger to patients is extremely low. USA TODAY

POPULAR STORIES

Apple Watch faces smartw competition from Fitbit, Ga and Samsung at IFA

usatoday.com | 10 hours ago

Daily Stormer neo-Na website owner once

25

# Over-the-Air Updates

Home › Mobile Security

## Over-the-Air Update Mechanism Exposes Millions of Android Devices

By Ionut Arghire on November 18, 2016

Tweet RSS

**The insecure implementation of the OTA (Over-the-air) update mechanism used by numerous Android phone models exposes nearly 3 million phones to Man-in-the-Middle (MitM) attacks and allows adversaries to execute arbitrary commands with root privileges.**

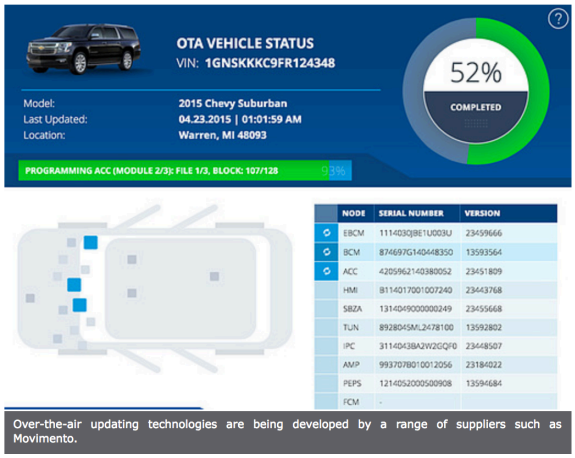
The vulnerable OTA update mechanism is associated with Chinese software company **Ragentek Group**, which didn't use an encrypted channel for transactions from the binary to the third-party endpoint. According to security researchers at AnubisNetworks, this bug not only exposes user-specific information to attackers, but also creates a rootkit, allowing an adversary to issue commands that could be executed on affected systems.

26

# Over-the-Air Updates for Cars!

**OTA updating brings benefits, challenges**

14-Aug-2016 03:23 EDT




Over-the-air updating technologies are being developed by a range of suppliers such as Movimento.

27

# Self Driving Tesla

## *Self-Driving Tesla Was Involved in Fatal Crash, U.S. Says*

By BILL VLASIC and NEAL E. BOUDETTE JUNE 30, 2016

A Tesla Model S, with its self-driving mode enabled. In a statement, the National Highway Traffic Safety Administration said it had sent an investigative team to examine the vehicle and the crash site in Williston, Fla. Jasper Juinen/Bloomberg

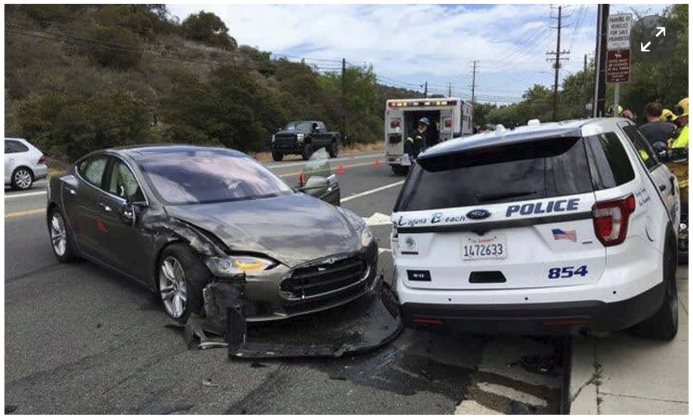
DETROIT — The race by automakers and technology firms to develop self-driving cars has been fueled by the belief that computers can operate a vehicle more safely than human drivers.

But that view is now in question after the revelation on Thursday that the driver of a Tesla Model S electric sedan was killed in an accident when the car was in self-driving mode.

28

# Tesla Autopilot Again

**If confirmed, it would be the third time a Tesla in autopilot has crashed into a stationary emergency vehicle this year**




▲ Photo provided by Laguna Beach police shows a Tesla sedan that crashed into a parked police cruiser on Tuesday. Photograph: AP

29

# Uber Self-driving Car


Photo by Vjeran Pavic / The Verge

Uber has discovered the reason why one of the test cars in its fledgling self-driving car fleet struck and killed a pedestrian earlier this year, according to *The Information*. While the company believes the car's suite of sensors spotted 49-year-old Elaine Herzberg as she crossed the road in front of the modified Volvo XC90 on March 18th, two sources tell the publication that the software was tuned in such a way that it "decided" it didn't need to take evasive action, and possibly flagged the detection as a "false positive."

30

# A Taste of Challenges

Taken on a recent trip between Toronto and Kingston

Scary! Especially when you consider what Machine Learning may decide to do in this situation

31

# A Taste of Challenges

What was really happening ☺

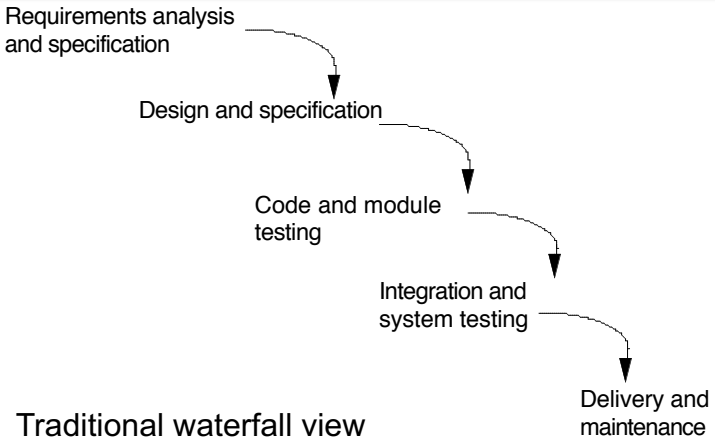
32

# The Bottom Line
# - My Opinion -

- It is no longer a question as to whether or not we can build the required software systems
- It is:
  - HOW CAN WE BUILD COMPLEX SOFTWARE INTENSIVE SYSTEMS SO THAT THEY ARE SAFE, SECURE AND DEPENDABLE
- That's really what this course is about – focused on embedded (medical) devices

33

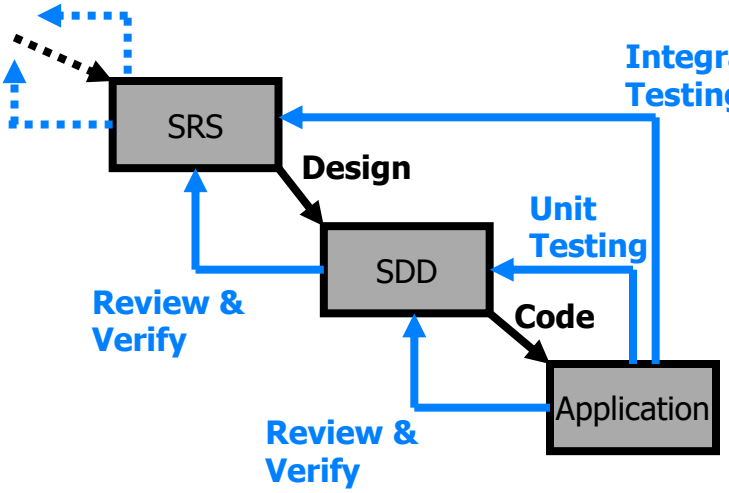
# The (traditional) software lifecycle - 1




Traditional waterfall view

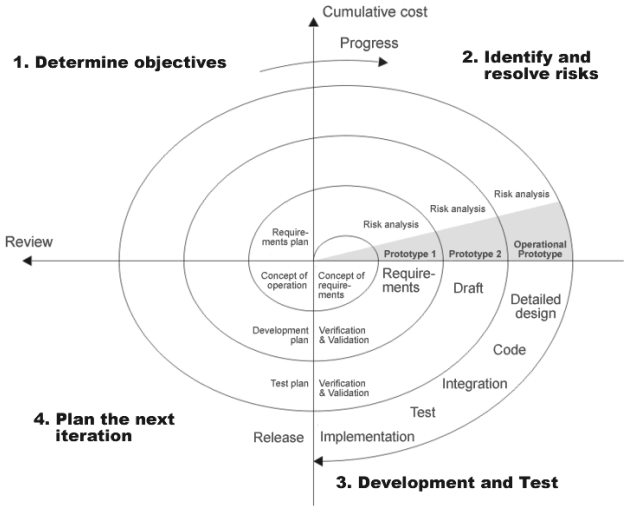
34

# The (traditional) software lifecycle - 2




35

# The (traditional) software lifecycle - 3




*Spiral model: Boehm 1988*



# Modern Trends

- Agile
  - Full-disclosure
    - At the moment I do not trust it for developing dependable, safe & secure systems
- Model-Driven Engineering
  - Likely to be THE development methodology for the foreseeable future

# Model-Driven Development The start

- The idea of model-driven (software) development originated many years ago, (at the time called “case tools”), but only relatively recently has it become a reality – and (my opinion) the future predominant way of developing complex systems
- Models have been in use for decades in engineering and science – so this is a natural progression

38

# Model-Driven Development (MBD) - 1

- Goes by many names (sometimes they mean something subtly different (including)
  - Model-Driven Engineering
  - Model-Based Design
- Basic idea:
  - Models of the system you want to build – and its environment
  - Transformation of system model(s) through various phases, until we can generate implementations (mechanical/electrical artifacts, code or other logic implementation)

39

# Model-Driven Development (MBD) - 2

- Benefits
  - Many types of analyses can be performed on the models to validate the initial model
  - Correctness-by-construction all the way through to implementation
  - Can also generate “proofs” or at least, checks, that correctness-by-construction is achieved
  - Can construct tools to help examine the models
  - Can regenerate implementations when changes are introduced

40

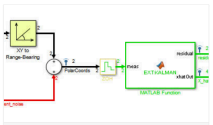
# Model-Driven Development (MBD) - 3

- Modern model-driven tool suites
  - Most common one in North America and world-wide for automotive and avionics is Matlab/Simulink, developed by The MathWorks
  - Others include IBM Rational, and mainly in Europe, SCADE, and ANSYS
  - We are going to explore/use Matlab/Simulink
  - Note: Simulink is really a design environment. The constructs in the language are focused on design rather than requirements – it is important to realize and remember this!

41

# Simulink – from the MathWorks Web Site

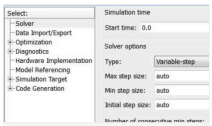
## Capabilities



### Building the Model

Model hierarchical subsystems with predefined library blocks.

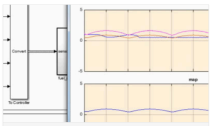
» Learn more



### Simulating the Model

Simulate the dynamic behavior of your system and view results as the simulation runs.

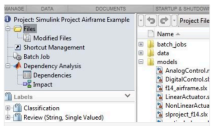
» Learn more



### Analyzing Simulation Results

View simulation results and debug the simulation.

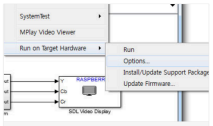
» Learn more



### Managing Projects

Develop and share applications as code, executables, or software components.

» Learn more




### Connecting to Hardware

Connect your model to hardware for real-time testing and embedded system deployment.

42