

**SE 2AA4, CS 2ME3 (Introduction to Software
Development)**

Winter 2018

02 Software Engineering Profession (Ch. 1)

Dr. Spencer Smith

Faculty of Engineering, McMaster University

January 9, 2018



02 Software Engineering Profession (Ch. 1)

- Administrative details
- What is Software Engineering (SE)?
- The PEO
- Historical origins of SE
- Software engineering in system design
- Examples of software failures
- The great gulf
- Challenges and opportunities for engineering
- Attributes of a good software engineer
- Software development process

Administrative Details

- GitLab access
- Tutorials this week (bring laptop)
- A1 changes
 - ▶ del method renamed rm
 - ▶ dunder
 - ▶ L^AT_EX

Software Engineering versus Computer Science

What is the difference between Software Engineering and Computer Science?

SE versus CS

- CS is the applied science for SE
- CS for theory, models
- SE applies theory and models
- SE associated with large, complex software
- SE associated with design and documentation
- SE associated with project management
- SE associated with real time embedded systems
- SE has an explicit ethical component
- Really a continuum

What is Software Engineering (SE)?

- Engineering for the development of software systems that
 - ▶ Are large or complex
 - ▶ Exist in multiple versions
 - ▶ Exist for large period of time
 - ▶ Are continuously being modified
 - ▶ Are built by teams
- “Application of a systematic, disciplined, quantifiable approach to the development, operation and maintenance of software” (IEEE 1990)
- “Multi-person construction of multi-version software” (Parnas 1978)
- Like other engineering areas, SE relies on mathematical techniques, especially logic and discrete mathematics
- Analogous to other engineering disciplines

Interesting Article

Programmers Should Not Call Themselves Engineers

PEng

How do you get an Engineer's Seal? Iron Ring?

The PEO (Professional Engineers Ontario)

- Degree from an accredited program (or a series of examinations)
- Experience requirement
- Law exam
 - ▶ Contracts
 - ▶ Torts
 - ▶ Exculpatory evidence
 - ▶ ...
- Code of ethics
 - ▶ Duty to society
 - ▶ Duty to employer
 - ▶ Duty to profession
- PEO protects the term Software Engineering
- The debate on SE in Canada started years ago

Software Engineering in System Design

- Embedded systems control physical systems
- Often makes SE a crucial part of system design
- Examples of embedded systems
 - ▶ Cell phones
 - ▶ Nuclear power plants
 - ▶ Automobiles
 - ▶ Aircraft
 - ▶ Pacemakers
 - ▶ mp3 players
 - ▶ Programmable household devices
- Embedded systems are rapidly appearing everywhere
- The developers of software for an embedded system needs to understand both the software and the physical device

Example Failures

What are some examples of software failures that you are aware of?

Example Failure: Therac-25

- The Therac-25 was a radiation therapy machine for treating cancer
 - ▶ Produced by the Atomic Energy of Canada Limited (AECL)
 - ▶ Controlled by software
- How it worked
 - ▶ Provided both electron beam and X-ray treatment
 - ▶ The machine produced low to high energy electron beams
 - ▶ X-rays were produced by rotating a target into the path of a high energy electron beam
- Used in several clinics across North America

Therac-25 Continued

- In six separate incidents in the 1980s, Therac-25 machines delivered overdoses of radiation causing severe physical damage or even death to the patients being treated
 - ▶ The second incident, which took place in Hamilton, resulted in administration of 13 000 – 17 000 rads of radiation (200 rads is regular treatment and 1000 rads can be fatal)
 - ▶ Three patients ultimately died from radiation poisoning
- What went wrong
 - ▶ Software failed to detect that the target was not in place
 - ▶ Software failed to detect that the patient was receiving radiation
 - ▶ Software failed to prevent the patient from receiving an overdose of radiation

Therac-25 Continued

Causes of failure

- Inadequate software design
- Inadequate software development process
 - ▶ Coding and testing done by only one person
 - ▶ No independent review of the computer code
 - ▶ Inadequate documentation of error codes
 - ▶ Poor testing procedures
 - ▶ Poor user interface design
- Software was ignored during reliability modelling
- No hardware interlocks to prevent the delivery of high-energy electron beams when the target was not in place

Example Failure: Public Servants Waiting for Pay

System glitch, or management problem?

Example Failure: 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.

Example Failure: 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.

Example Failure: 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.

Example Failure: 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.

Example Failure: 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.

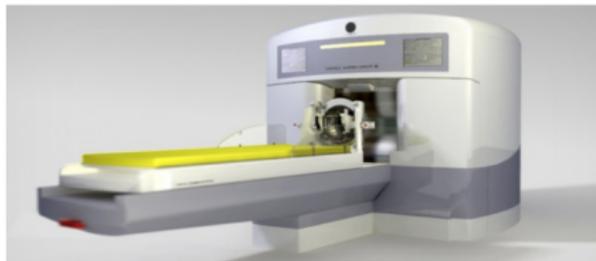
According to a letter sent to its Canadian customers, Baxter has received reports of incidents where the COLLEAGUE triple channel infusion pumps stopped infusing. According to the "Urgent Device Correction" notice issued by Baxter, the company is working on a software solution to fix the problem with 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.

Example Failure: 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

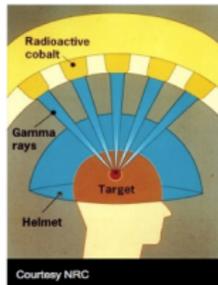
dig it

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.



Courtesy NRC

Example Failure: 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.

Example Failure: Radiation Overdose

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.

[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.

 SIGN IN TO E-MAIL

 PRINT

 SINGLE PAGE

 REPRINTS

 SHARE



Example Failure: Radiation Overdose 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.

[Enlarge This Image](#)



Marci Faber is nearly comatose after a treatment mistake.

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.

[RECOMMEND](#)

[TWITTER](#)

[COMMENTS](#)
(185)

[SIGN IN TO E-MAIL](#)

[PRINT](#)

[SINGLE PAGE](#)

[REPRINTS](#)

[SHARE](#)



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.

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



Example Failures?

Was y2k a Software Failure? Did anything bad happen?

For more on y2k, see [Parnas, 1999](#)

Would you Trust Software to Guide a Missile Defence System?

History

- The field of software engineering was born in 1968 in response to chronic failures of large software projects to meet schedule and budget constraints
- Recognition of “the software crisis”
- Term became popular after NATO Conference in Garmisch Partenkirchen (Germany), 1968

The Great Gulf

- Engineers do not sufficiently understand or care about software
 - ▶ Many of the basic principles of software design and development are largely unknown to engineers
 - ▶ Engineers often do not appreciate the challenges and dangers inherent in software for embedded systems
- Software developers lack engineering training and professionalism
 - ▶ There is an entrenched culture of producing software without any guarantee whatsoever
 - ▶ There is no system for certifying either software or software developers
 - ▶ Most software developers lack the engineering background needed to produce software for embedded systems

Challenges and Opportunities for Engineering

- Challenges
 - ▶ Engineers need to design systems that have safe, correct, high-quality software
 - ▶ Software engineers need to produce software that they can guarantee
 - ▶ No silver bullets
 - ▶ Maturing, but still an immature field
- Opportunities
 - ▶ Software tools can greatly enhance the capabilities of engineers
 - ▶ Software can greatly increase the effectiveness of the devices engineers design

Attributes of a Good Software Engineer

What are the attributes of a good software engineer?

Attributes of a Good Software Engineer

- Is a good engineer!
- Embraces
 - ▶ Rigour
 - ▶ Being systematic
 - ▶ Documentation
 - ▶ Specification
 - ▶ Mathematics
 - ▶ Evidence (measurement) based decisions
 - ▶ Ethics
 - ▶ Professionalism
- Can program in the large as well as in the small
- Has a solid understanding of computing and software
- Comfortable with different levels of abstraction
- Communicate and work effectively with a team
- Management skills

Software Development Process

- A rational development process is needed to produce quality software
- Any proposed rational process is necessarily an idealization
 - ▶ Humans inevitably make errors
 - ▶ Communication between humans is imperfect
 - ▶ Many things are not understood at the start
 - ▶ Supporting technology always has limitations
 - ▶ Requirements change over time

Software Lifecycle

