SFWRENG / MECHTRON 3K04 Software Development

Welcome! Move to the closer tables, this is a very big room ☺

McMaster University
Engineering
Computing & Software

September 3rd, 2025

Dr. Angela Zavaleta Bernuy

About me!

- I am an Assistant Professor, Teaching Track in the Department of Computing and Software
- Background:
  - 2015-2020: B.Sc. in Computer Science and Mathematics at the University of Toronto Scarborough
  - 2020-2022: M.Sc. in Computer Science at the University of Toronto
  - 2022-2025: Ph.D. in Computer Science at the University of Toronto
- It is my first time teaching at McMaster!
- How to address me: Dr. Zavaleta, Prof. Zavaleta, Dr./Prof. Angela
- How not to address me: Ma'am, dude, bro, %@&!
- Interests: Traveling, cooking/baking, board games, Lego

Research Interests

- Computing Education Research (CER or CS Ed)
  - How can we support student's learning in computing courses?
  - How can we improve the student experience in computing courses?
  - **How can we train students for the real-world and equip them with technical and non-technical skills?**
  - How can we *really* understand students?!
- Human-Computer Interaction (HCI)
  - How do humans interact with our tools?
  - How can we improve the user experience?
- Research Methods
  - How do we conduct and report research?

About you!

- Around 40% of you are in Mechatronics and 60% of you are in Computer Engineering
  - Some of you also have health or management backgrounds
  - For the majority of you, this is your first software development course
- What are you worried about?
  - Time management / workload
  - Learning curve
  - Finding a team
  - Connection between the lecture and the project
- What are you excited about?
  - The project: learning new skills, working as a team, improving quality of work, etc.

About this course!

- A hands-on overview of system development, model-driven engineering, and assurance for safety critical software systems.
- We are going to cover…
  - Software requirements
  - Hazard analysis
  - Software design
  - Implementation
  - Verification and validation
  - Development and testing
  - Safety and security
- The project will focus on safe, secure and effective medical devices.

Course Information

- The course page is in Avenue to Learn
  - The syllabus and course policies are posted – read these carefully for important admin details!
- All the deadlines have been added to the Avenue to Learn calendar, including office hours.
  - We will keep adding office hours closer to important deliverables.
- 3 hours of lecture every week
  - You *should* attend ☺
- 3 hours of labs every week
  - You **must** attend!

Application of

Methods and long-term knowledge

To build skills

Teaching Assistants

- Vasily Kapustin
- Marwan Madkour
- Pedro Neto
- Mohamadreza Sabeghi
- Hamza Siddiqui
- Sameer Suleman

Course Breakdown

Assessment of Learning	Number	Weight
Project	2	40%
Midterm Test (In class: Wednesday, October 22nd)	1	25%
Final examination (tests cumulative knowledge)	1	35%
BONUS: Research surveys	2	1%
	TOTAL	100%

If your final examination grade is **higher** than your midterm test grade, **your final examination grade will replace your midterm test grade**.

Project

- One project split into two deliverables
- The project is in teams of 5-6 students from **the same lab**
- Each deliverable will have various components: code, documentation and demo to the TA.
- Deliverable 1:
  - Due: Monday, October 27th at 8am
  - Demo: Monday, October 27th to Friday, October 31st in the lab
- Deliverable 2:
  - Due: Monday, November 24th at 8am
  - Demo: Monday, November 24th to Friday, November 28th in the lab
- Project details will be posted soon!

Midterm Test and Final Examination

- The midterm test will be 45 minutes and will be written on paper in person
  - Date: **Wednesday, October 22nd, 2025 at 5:30pm**
  - Location: PGCLL-M21
  - More information will be posted later on.
- The final examination will be 3 hours and will be written on paper in person
  - It will be scheduled later in the term by the registrar
  - It will be cumulative
  - More information will be posted later on.

Academic Integrity

- Everything you (and your team) submit must be your own work
  - Not another team, not another student from last term, not a tutor, not an online source, …
- Never look at another solution or share your own solution
- It's okay to discuss parts you are stuck with, but do not look at each other's implementation
- Generative AI policy:
  - The goal of this course is for you to learn comprehensive software development topics
    - LLMs are most likely not experts in everything you will see in the course, be careful!
  - If you use it in your deliverables, you should explain how you did so in your submission
  - If you use it for understanding or practicing a concept, double-check the sources.

What can you expect of us?

- Clear and regular communication
- Course material designed and regularly improved to give you the best learning experience we can
- Lots of opportunities for help in lecture and office hours
- Coursework posted on time and marked with constructive feedback
- Safe space to ask questions

What we expect of you?

- Respect the teaching team and your fellow classmates
- Keep up with the lecture and lab content
  - Everyone behind you or next to you can see your computer screen
  - Don’t be that person: don’t watch videos, don’t play games, don’t scroll on anything
  - Use your devices to enhance your learning!
- Try it out before asking for help
  - The journey of collaborating to arrive to the solution can be very rewarding!
  - If you are stuck, don’t be afraid to ask
- Don’t cheat, copy, plagiarize… there is always a better way!
- Help us help you: we are all trying our best! Feedback is always welcome, but keep it constructive!

Getting help

- Course discussion forum:
  - We will use Teams as a discussion forum
  - Post questions about course material that other students may also be interested in:
    - Ask if you are confused
    - Answer other students if you know the answer
  - Do not post solutions (or partial solutions) to marked coursework before the deadline!
- For matters that pertain only to you, you can send an email directly to me or attend office hours for 1-1 help.
- Office hours:
  - Held in-person or virtually every week, check the course calendar!
- Email:
  - Add **[3K04]** in the subject line.

Course content questions won't be answer through email!

The Role of Software

Most of the systems we are interested these days are **software-intensive**

↓

We need to pay **special attention to software** even though we are eventually **interested in the system**

Software Engineering: Past Knowledge

- Application of engineering to software
- Built on mathematics and computer science
- Real-world software is:
  - Large and complex
  - Built by teams
  - Versioned
  - Long-lived
  - Evolving

- Application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software (IEEE 1990)
  - IEEE Standard Glossary of Software Engineering Terminology
- Multi-person construction of multi-version software

Software Engineering in System Design

- Software engineering often fits inside bigger systems
- Embedded software:
  - 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

Examples:
Software Failures

Health-care Database (2005)

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.

Defibrillator Recall (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.

Defibrillator Recall (2025)

HEALTH

FDA flags problems with two Boston Scientific heart devices tied to injuries and deaths

WASHINGTON (AP) — U.S. health regulators are warning doctors and patients about safety issues with two separate Boston Scientific heart devices recently linked to injuries and deaths.

The Food and Drug Administration issued two alerts Wednesday about electrical problems tied to the company's heart-zapping defibrillator systems and a separate issue with a heart implant used to reduce stroke risk.

The agency said some of the company's Endotak Reliance defibrillator wires can become calcified, leading to failures in delivering life-saving shocks to the heart, according to the FDA.

Defibrillators are surgically placed in the upper chest, where they monitor irregular heartbeats and use electrical shocks to jolt the heart back to normal.

As of July 24, Boston Scientific has reported 386 serious injuries and 16 deaths associated with this issue, the agency said.

Gamma Knife (2009)

‘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.

Courtesy NRC

Radiation Overdose (2010)

Radiation Offers New Cures, and Ways to Do Harm

By WALT BOGDANICH
Published: January 23, 2010

SIGN IN TO E-MAIL
PRINT
SINGLE PAGE
REPRINTS
SHARE

JEFF BRIDGES MAGGIE GYLLENHAAL
CRAZY HEART
NOW PLAYING
IN SELECT THEATERS
WATCH TRAILER

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.

THE RADIATION BOOM

A Pinpoint Beam Strays Invisibly, Harming Instead of Healing

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

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

CEDAR RAPIDS
COMING SOON

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.

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.

Infusion Pumps (2007)

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.

Infusion Pumps (2025)

Zyno recalls infusion pumps over unvalidated software

Customers have been asked to stop using the pumps and wait for someone to contact them about exchanging devices.

Dive Brief:

- Zyno Medical has recalled infusion pumps that shipped with software that had not undergone verification and validation testing, the Food and Drug Administration said Monday.
- The company released the Z-800 pumps with incorrect software versions. The software created a risk of incorrect air-in-line detection and audio alarms that could cause serious harm.
- Zyno has not reported any serious injuries or deaths. The recall, which the FDA assigned to Class I, started eight months after Zyno removed Z-800 pumps from use over another software issue.

Pacemaker Security (2016)

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.

Pacemaker Security (2017)

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

Pacemakers: What else could go wrong?

- What are some features of a pacemaker that could fail?
  - You don't know much about pacemakers? That's okay!
  - What is potential edge case that could be dangerous if it isn't tested?
- Discuss with your table
- Then, share with the class.

Pacemakers and iPhones (2021)

Healthcare IT News TOP

Global Edition Medical Devices

FDA warns of pacemaker-iPhone interference

A new study tested the static magnetic fields of iPhone 12 models and the Apple Watch in an attempt to determine their minimum separation distance from implanted medical devices.

By Kat Jercich | August 26, 2021 | 04:56 PM

Insulin Pump Security (2016)

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

Over-the-Air Updates (2016)

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.

Over-the-Air Updates for Cars (2016)

Self-Driving Cars (2016)

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.

Self-Driving Cars: Uber's Crash (2018)

INNOVATION > SCIENCE

Who Is Responsible In A Crash With A Self-Driving Car?

On March 18, 2018, at nearly 10 PM, a self-driving Volvo hit and killed a pedestrian, a woman named Elaine Herzberg. Herzberg's death was the first pedestrian fatality involving a self-driving car. The self-driving car was a test vehicle, a car that Uber was testing in Arizona. It could not figure out if the woman was a pedestrian, a bicycle, or another car, nor predict where she was going. Video showed that the driver of the self-driving car, acting as a "safety backup", was not looking at the road at the time of the collision. Instead, she was watching an episode of "The Voice".

In this March 20, 2018, file photo provided by the National Transportation Safety Board, investigators examine a driverless Uber SUV that fatally struck a woman in Tempe, Ariz. A prosecutor has determined that Uber is not criminally liable in the crash that killed 49-year-old Elaine Herzberg. (National Transportation Safety Board via AP, File) Less

ASSOCIATED PRESS

Self-Driving Cars: Tesla's Crash (2025)

Tesla hit with $243 million in damages after jury finds its Autopilot feature contributed to fatal crash

The verdict follows a three-week trial that threw a spotlight on how Tesla and CEO Elon Musk have marketed their driver-assistance software.

MIAMI – A federal jury on Friday found Tesla partly liable in a 2019 car crash that killed a pedestrian and left another person badly injured when the car was in Autopilot mode.

The jury awarded the plaintiffs $43 million in compensatory damages for pain and suffering plus $200 million in punitive damages, which are intended to deter future harmful behavior by Tesla.

The verdict is a blow for Tesla and CEO Elon Musk as they try to convince the public, government regulators and investors that their self-driving software is safe.

The eight-person jury said that Tesla was partly to blame for the crash in the Florida Keys six years ago, when neither the driver of the Tesla sedan nor the Autopilot software braked in time for an intersection. The jury assigned Tesla one-third of the blame and assigned two-thirds to the driver, who was reaching for his cell phone at the time of the crash. He was sued separately.

Self-Driving Cars: Waymo (2025)

Self-Driving Cars: Waymo (2025)

Self-Driving Cars: Challenges

Self-Driving Cars: Challenges

Takeaways

- It is no longer a question as to whether or not we can build the required software systems…
  - … because, we can!
- It is

How can we build complex software intensive systems so that they are **safe**, **secure** and **dependable**?

- This is what the course is about!
- We will focus on embedded medical devices
- Another challenge: How do we demonstrate safety of systems that employ machine learning components?

McMaster University | Engineering

Visit our engineering grad studies fair!

Interested in exploring graduate studies after you graduate? Visit our upcoming fair to meet with staff, students, and faculty from across Canada!

September 18, 2025

1:00 p.m. - 4:00 p.m.

JHE Lobby

Scan to learn more

Brighter World

Next Week!

- Project overview:
  - Two TAs will attend lecture to share their experiences as students and as TAs
- Challenges and complexities in Software Engineering