Dependability

Outline of the course

- Basic terms and taxonomy of dependable and secure computing
- Redundancy in fault tolerant computing
- Quantitative evaluation of dependability
- Software reliability
- Risk analysis
- Security issues
- Road vehicles:Functional safety and Road vehicles: Cybersecurity engineering
- Cyber-physical systems modelling and simulation

- Hands on activities

  - Mobius tool, PVS tool and INTO-CPS tool

Instructor Dr. Maurizio Palmieri, Department of Information Engineering
maurizio.palmieri@ing.unipi.it

Dependability

Tools

1. install virtual box from the homepage: https://www.virtualbox.org/wiki/Downloads
2. download the VM from: http://www.iet.unipi.it/c.bernardeschi/didattica/FMSS
   in which Mobius, PVS and INTO-CPS are already installed
3. Follow the following instructions to obtain a license for the Mobius tool

Instructions to obtain the Mobius tool

1. Visit http://www.mobius.Illinois.edu
2. Click "Login" in the menu bar
3. In the login page, click "Create an account"
4. Follow instructions to obtain a license. In particular,
   a) use the institutional unipi.it email address
   b) In a comment field, say that you are attending a course on dependability held by prof. Cinzia Bernardeschi (owner of an academic license)
5. Within 48 hours, you should receive a confirmation letter with the link to get the license (and to download the tool)
6. Versions of the tool are available for Ubuntu Linux, Mac OSX, and Windows either 32 or 64 bit

Dependability

From Wikipedia:

In systems engineering, **dependability** is a measure of system’s **availability**, **reliability**, **maintainability**, and in some cases, other characteristics such as **durability**, **safety** and **security**

Dependable computer-based systems

In real world, dependability problems are really subtle.

- There is a root cause that evolves.
  Something happens in a subsystem, something else happens in another subsystem, …., and then we have a failure.
- System are designed to ensure within a given operational conditions.
  It is very hard to anticipate the operational conditions correctly.
- The occurrence of failures is very complicated to avoid.
- In many cases fault tolerance can be useful.

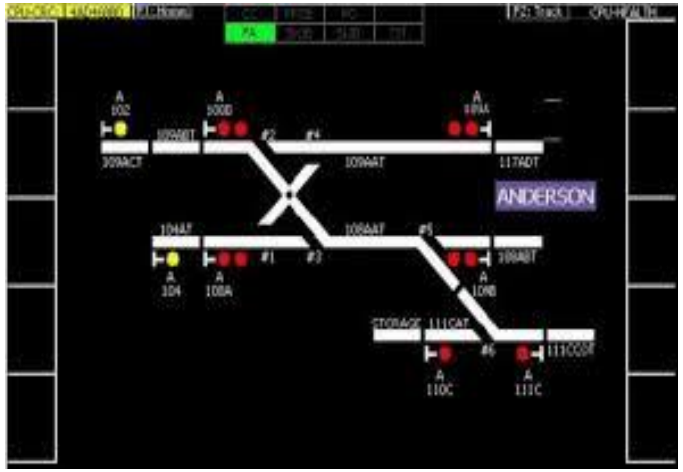
Dependable computer-based systems

- In safety critical systems community, people are forced to document and publish the problems (accidents)
- You have to publish problems, to document them, to analyse them to be sure that nobody else has the same problem again
- In this way, data for dependability research can be collected and analysed to learn

- General questions:
  - how to build dependable computer-based systems?
  - can we justifiably trust the dependability of such systems?

Examples of computer-based safety-critical systems

Transport systems : Railway Interlocking system

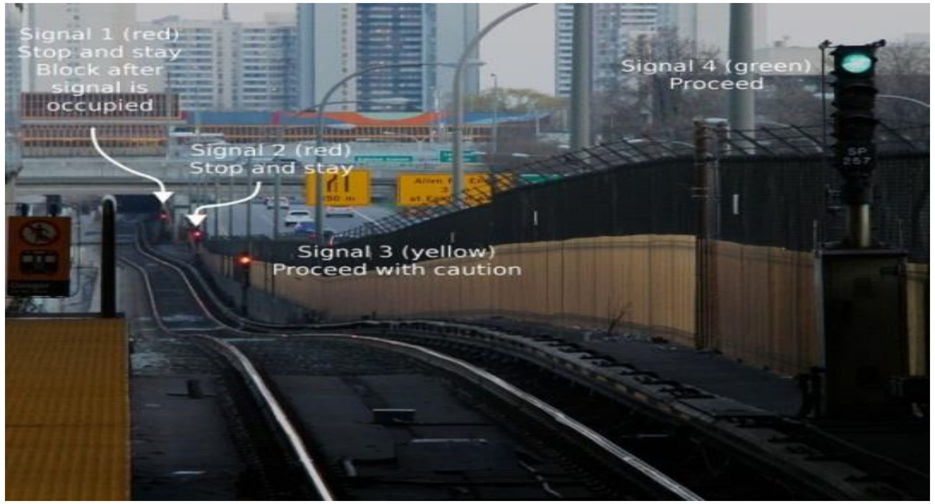


Interlocking: arrangment of signals for safe movement of trains over tracks

From mechanical interlocking (route settings by levers)
to electrical (electro-mechanical) intelocking
to electronic/computer-based interlocking

Computer-based interlocking:

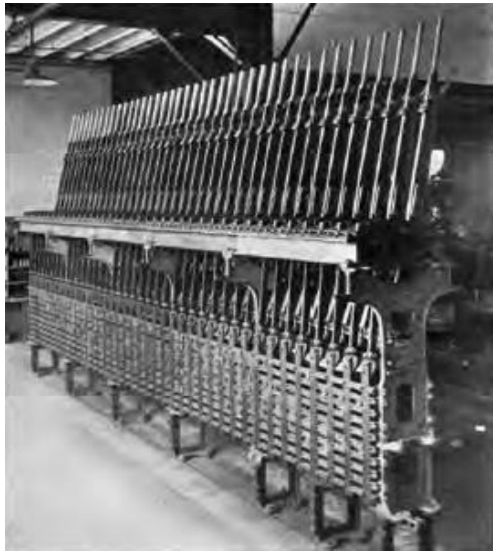
- software logic running on special-purpose control hardware
- logic is implemented by software rather than hard-wired circuitry
- facilitates modifications by reprogramming rather than rewiring



Signal blocks on a subway system (Toronto) : 4 signals , short blocks
If a train has just passed the most distant signal, the two most distant signals are red (*stop and stay* aspect);the next closest signal is yellow (*proceed with caution*), and the nearest signal shows green (*proceed*).

https://en.wikipedia.org/wiki/Signalling_of_the_Toronto_subway

Transport systems: Railway Interlocking system



Mechanical control (leavers)

King, Everett E. - "Railway Signaling." (New York:McGraw-Hill.

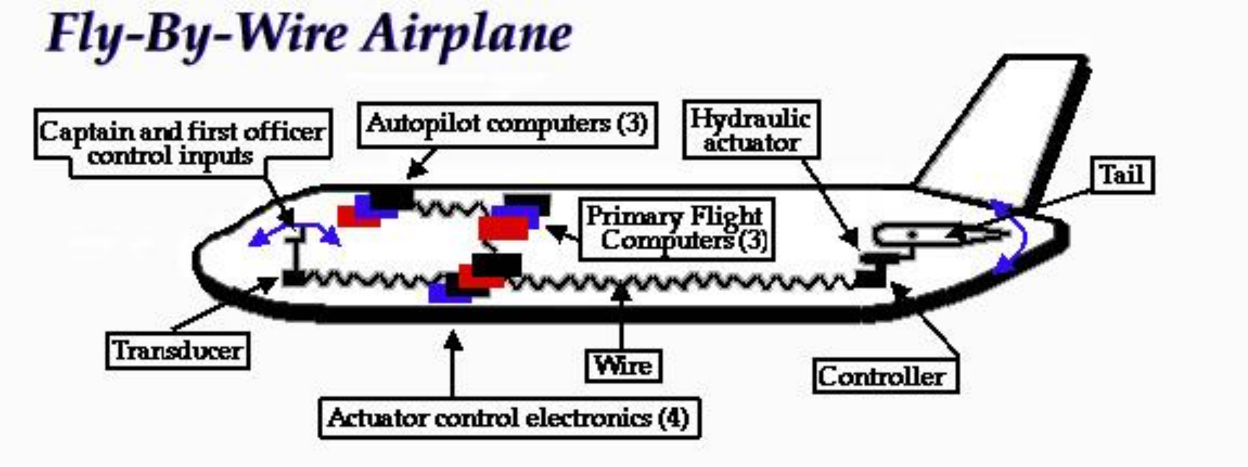
Levers operate the field devices, such as signals, directly via a mechanical rodding or wire connection

Computer-based controls

Supervisory control and data acquisition (SCADA) systems to view the location of trains and the display of signals.

Electro-mechanical control
Railway station on the Verona-Bologna track
Interlockings using electric motors for moving switches and signals

Transport systems: Aerospace


Fly-By-Wire Airplane
Captain and first officer control inputs
Autopilot computers (3)
Hydraulic actuator
Tail
Primary Flight Computers (3)
Transducer
Wire
Controller
Actuator control electronics (4)

Boeing's first attempt at a completely fly-by-wire commercial airplane.
Source: https://www.mura.org/websites/me39c.me.berkeley.edu/Spring97/Projects/b777/flightdeck2.html

Earliest aircrafts: mechanical and hydro-mechanical flight control system; series of levers, rods, cables, ….

Fly-by-wire (FBW) system: all commands and signals are transmitted electrically along wires. The pilot uses a console.

These signals are sent to **flight-control computers (FCS)** that reconvert the electrical impulses into instructions (to the actuators) for control surfaces, like wing flaps or the tail.

Fully fly-by-wire systems: devices in the control surfaces measure their position and transmit that data back to the flight computer. Flight computers can be programmed to carry out adjustments to control surfaces automatically in a control loop.

Transport systems: Aerospace

Air traffic Control

Source:http://www.adp-i.com/en/our-solutions/airport-expert-appraisals/air-navigation

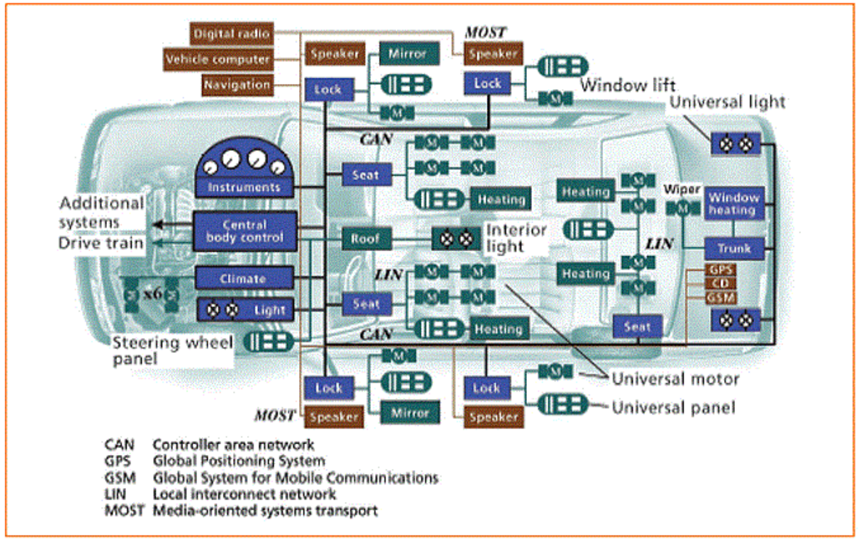
Air Traffic Control (ATC) is a service provided by ground-based controllers who are responsible for maintaining a safe and efficient air traffic flow.

ATC is transitioning to use of the Global Positioning System for Navigation and precision approaches

Future generation of ATC: **Airborne Self-Separation**
an operating environment where pilots are allowed to select their flight paths in real-time.

Main challenge:
coordination between aircrafts within a dynamic environment, where the set of surrounding aircraft is constantly changing.

Transport systems: Automotive



Drive-by-wire

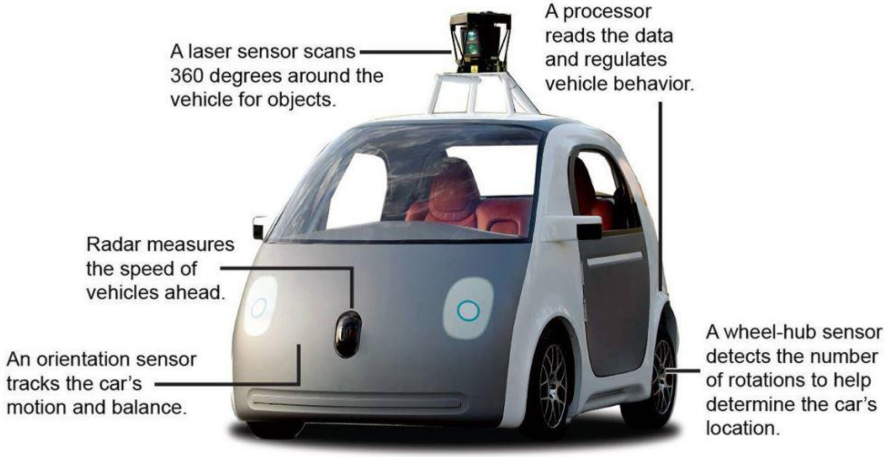
traditional mechanical control of vehicle functions replaced by ECUs

Over 80 different embedded processors, interconnected

Key ECUs (Electronic Control Unit):

- Engine Control Module (ECM)
- Electronic Brake Control Module (EBCM)
- Transmission Control Module (TCM)
- Vehicle Vision System (VVS)
- Navigation Control Module (NCM)
- …

Autonomous Vehicles (capable of sensing its environment and navigating without human input)



A laser sensor scans 360 degrees around the vehicle for objects.

A processor reads the data and regulates vehicle behavior.

Radar measures the speed of vehicles ahead.

An orientation sensor tracks the car's motion and balance.

A wheel-hub sensor detects the number of rotations to help determine the car's location.

Source: Google

Raoul Rañoa / @latimesgraphics

Array of sensors needed to provide the autonomous system with situational awareness about the physical world. Embedded processors use this information to make appropriate decisions about what actions the autonomous system should perform.

Digital Instrumentation and Control

Digital I&C: analog and mechanical parts are replaced by CPUs and software

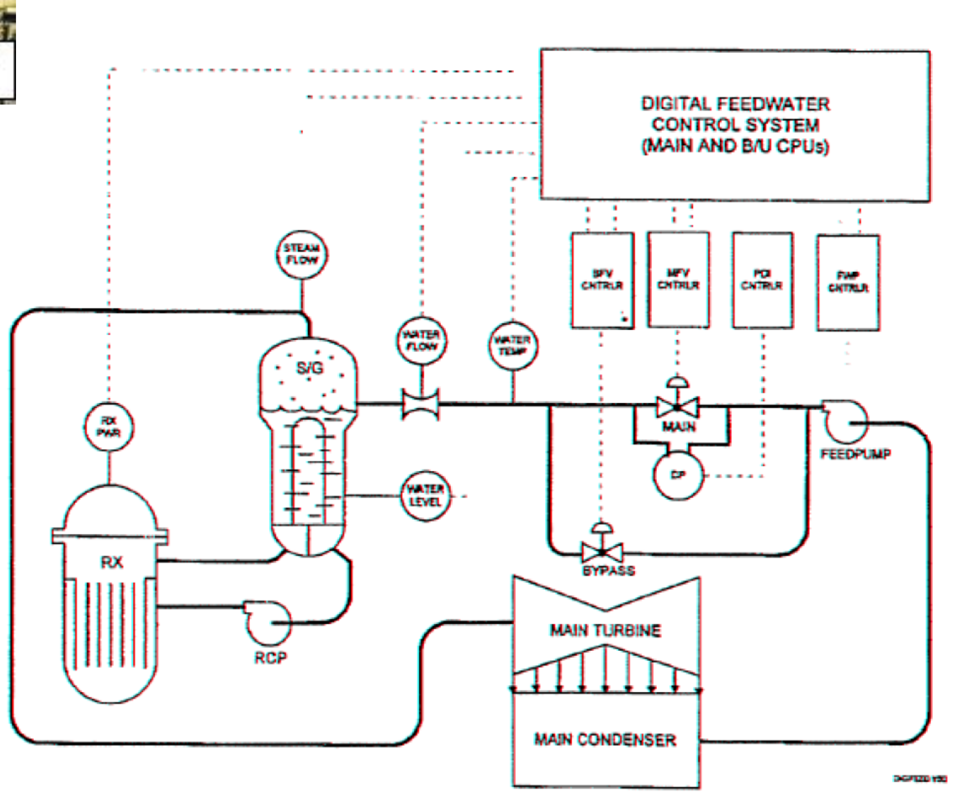
A Digital Control System samples feedback from the system under control and issues commands to the system in an attempt to achieve some desired behaviour

Nuclear Power Plant (NPP)

Reactor coolant loop:
- RX: reactor
- Reactor coolant pump (RCP)
- Steam Generator (S/G)

Main components of the FeedWater Systems (FWS)
- FWPs (FeedWater Pumps)
- MFRVs (Main FeedWater Regulating Valves)
- BPFRVs (Bypass FeedWater Regulating Valves)

Schematic of NPP digital feedwater control system



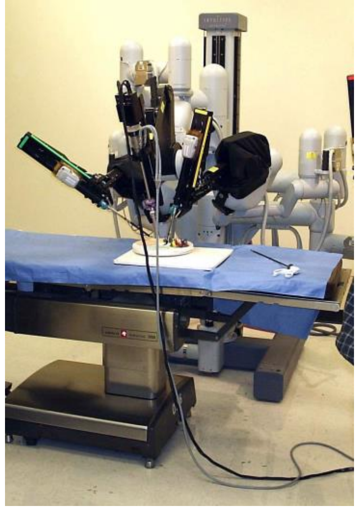
Source: ''Traditional Probabilistic Risk Assessment Methods for Digital Systems'', U.S. Nuclear Regulatory Commission, NUREG/CR-6962, 2008

Healthcare: Medical systems

PCA devices
A patient-controlled analgesia (PCA) infusion pump, configured for intravenous administration of morphine for postoperative analgesia, programmable thorugh an interactive user interface

Cardiac Pacemakers
The bulk of the device contains its battery and electronic control systems. The leads detect the heart's electrical activity, transmit that information to the pacemaker's electronics for analysis and, if the natural activity is deemed irregular, deliver an electrical charge from the pacemaker's batteries that causes the cardiac muscle to contract, pacing the pumping of the heart.

Robotic Surgical Systems
Da Vinci Surgical System: Approved by the Food and Drug Administration (FDA) in 2000, it is designed to facilitate complex surgery using a minimally invasive approach and is controlled by a surgeon from a console.



Source: http://www.davincisurgery.com/da-vinci-surgery/da-vinci-surgical-system/

Examples of safety-critical systems failures

Ariane 5 - Flight 501

Ariane 5 is one of a range of launch vehicles developed by the European Space (ESA), part of the Ariane rocket family

“ The morning of the 4th of June 1996 was partially cloudy at Kourou in Guyana as the European Space Agency (ESA) prepared for the first launch of the French-built Ariane 5 rocket. The rocket lifted off at 09:34. Just 37 seconds later, the rocket veered on its side and began to break up. The range safety mechanism identified the impending catastrophe and initiated explosive charges that blew up the rocket to prevent further damages and possible casualties. An investigation by the ESA determined that the accident was caused by a software ‘bug’. ”

The flight is known as flight 501.

The Bug That Destroyed a Rocket, Mordechai Ben-Ari. *SIGCSE Bulletin*, n. 2, 2008

The reason was that:
-the engines were gimbled to extreme positions and this caused the vehicle to pitch over.
-the pitch over led to excessive aerodynamic loads that caused the self-distruct mechanism to operate.

Ariane 5 - Flight 501

Investigation by inquiry board assembled by ESA and consisting of international experts.
Report: July 9, 1996

Many factors were involved in the accident, but one of the most important involved the software in part of the vehicle’s Flight Control System, called the Inertial Reference System (IRS).
IRS supplies velocity and angles from which calculations are computed that set the various control surfaces.

The goal was to keep the vehicle on the planned trajectory.

A sw component that is used for alignment while the vehicle is on the ground prior to lanch was still executing.
This was not necessary, but not viewed as a problem.

Written for Arian IV, such module was used on Arian V because the required functionality was similar.

The module calculated the value related to the horizontal velocity component, but this value was higher than the values in Arian IV.

Ariane 5 - Flight 501

The higher value was not representable in the available precision and that resulted in an exception being raised.

The exception handler was not provided for this situation and the exception was propagated according to the ADA exception semantics and this caused the execution of a significant amounts of the software to be terminated

In particular test bit patterns were sent to the engine control actuators rather that correct values.
This caused the vehicle to pitch over just prior to abrupt the end of the maiden flight.

There was a backup inertial system, but the backup system, an identical redundant unit, failed in the identical manner a few milliseconds before. It was running the same software.

ARIANE 5 Flight 501 failure, Inquiry Board Report, 1996
(http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html)

Ariane 5 - Flight 501

Remarks

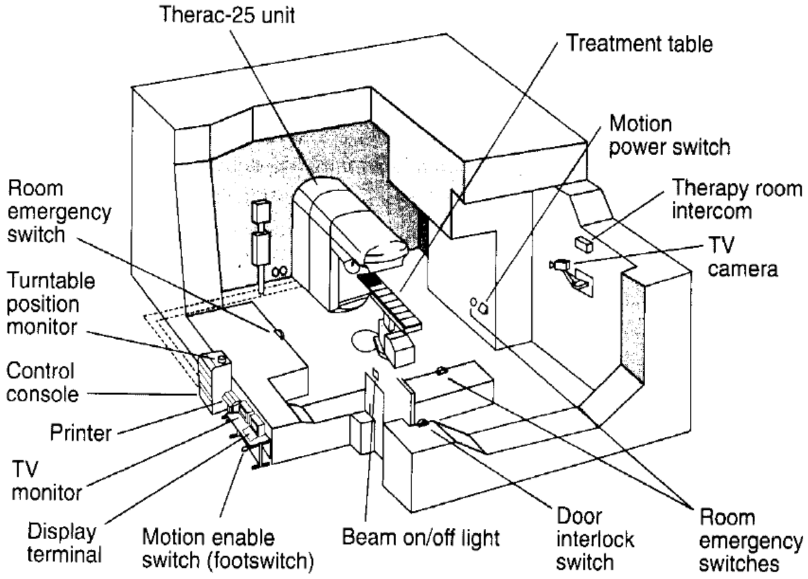
- In Arianne 5, they reused the same software but they replaced the sensors: “new sensor and old software that read these sensors”
- The old software was not able to deal with large numbers produced by new sensors, we had an overflow problem.
- This was never tested due to budget constraints.

- “The subsystem that had the problem was a part dedicated to align the system before lunch – it should have been turned off!”

Therac-25 radiation therapy machine

- Therac-25 is a machine for radiation therapy
  Atomic Enery of Canada Limited + French company
  It was involved in at least six accidents between 1985 and 1987, in which patients were given massive overdoses of radiation

https://en.wikipedia.org/wiki/Therac-25



- The machine sometimes gave its patients
  radiation doses that were hundreds of times greater than normal
- **Functional principle:**
- medical linear accellerators, accellerate electrons to create high energy beams that can destroy tumors with minimal impact on the surrounding healthy tissue.
- “scanning magnets” are used to spread the beam and vary the beam energy
- **Two operation modes:**

1) high power beam (X-rays, 25 MeV) ; 2) low power beam (electrons at various energy levels)

- **Accident:** high power mode (a lot of energy) without spreader plate activated -> caused by software flaws

Therac-25 radiation therapy machine

Previous machines: Therac-6 (one operation mode, X-rays) and Therac-20 (two operation mode, X-rays and electrons)

- sw functonality was limited in both machines
  (sw added convenience to the existing hardware, which was capable of standing alone)
  - Independent protective circuits for monitoring the electron-beam scanning plus mechanical interlocks for ensuring safe operations.

Therac-25 (AECL) :
- based on a new ''double pass'' concept of electron acceleration
- software more responsability for mainaining safety:
  computers used to control/monitor the hw and all the existing hw safety mechanisms and interlocks were not duplicated
- some sw of the previous machines was iter-related or reused

These accidents highlighted the dangers of software control of safety-critical systems, and they have become a standard case study in health informatics and software engineering

Therac-25 radiation therapy machine

- A turntable rotates accessory equipment into the beam path to produce the two therapeutic modes. A third position involves no beams and is used to correct positioning of the patient
- Among equipment:
  - scanning magnets are used to spread the beam to a safe therapeutic concentration. An ion chamber is used to measure electrons, and a beam flattener is used, in X-rays mode, to produce a uniform treatment field. The computer is responsible for the correct positioning of the turntable.
- in particular system states, software faults allowed X-rays operation mode in a wrong equipment setting. Moreover, in some cases the software interlock failed due to a race conditions.
- A commission concluded that the primary reason should be attributed to the bad software design and development practices, and not explicitly to several coding errors that were found. In particular, the software was designed so that it was realistically impossible to test it in a clean automated way
- Some information on Threac-25 software development process etc are not available.

Medical Devices: The Therac-25, Nancy Leveson, U. of Washington. In *Safeware: System Safety and Computers*, Addison-Wesley, 1995

Toyota Sudden Unintended Acceleration

https://www.viva64.com/en/b/0439/

Sudden Unintended acceleration (SUA) is one of the most deadly automotive defects in history.

"The issue became public in August 2009 after an accident in San Diego, Calif., killed a family of four. The mat entrapped the gas pedal, accelerating the car at full throttle. The incident occurred after the National Highway Traffic Safety Administration (NHTSA) had opened a defect investigation into the ES350 over that issue in 2007 and identified other Lexus models that might be similarly defective."

http://www.cbsnews.com/news/toyota-unintended-acceleration-has-killed-89/

"On August 28, 2009, California Highway Patrol Officer Mark Saylor, his wife, young daughter and brother-in-law died in a horrific crash, when the 2009 Lexus ES 350 Saylor had been driving, "failed to stop at the end of Highway 125."
According to the report filed a month later by NHTSA investigators, Saylor's Lexus, "entered the T-intersection and collided with a Ford Explorer. The Lexus continued on past the end of the T-intersection and struck an embankment, at which time it became airborne. The Lexus eventually came to rest in a dry riverbed where it burned for an extended period of time."

Toyota Sudden Unintended Acceleration

- Since 2003, NHTSA’s Office of Defect Investigations (ODI) has opened eight separate investigations into allegations of Sudden Unintended Acceleration. Most have been very brief and closed with no defect finding. The only cause the agency has ever found for Toyota SUA has been **pedal interference caused by floor mats**.
- Toyota had successfully responded by denying that any problem existed – it blamed consumers for installing accessory floor mats that could entrap the accelerator pedal and agreed to replace the mats, or post warnings.
- This remedy had satisfied NHTSA

BUT the moments before the Salylor crash were captured in a frantic and publicly broadcast 911 call, by describing panic in a runway vehicle

Many could not understand why a highly experienced California Highway Patrol officer couldn’t safely bring the vehicle under control and to a stop.

Sean Kane, Ellen Liberman, Tony Di Viesti, Felix Click. Safety Toyota Sudden UnintendedAcceleration, Safety Research & Strategies, Inc., 2010, http://www.safetyresearch.net/Library/ToyotaSUA020510FINAL.pdf

Toyota Sudden Unintended Acceleration

ʻʻ Sudden unintended acceleration is a complex problem. There are multiple causes that can result in a vehicle accelerating without the driver’s intent:

design defects which induce driver error – such as poor pedal placement, the lack of a shift interlock, floor mat interference, or mechanical or electromechanical defects and electronic defects.

The latter –which is the most difficult to pinpoint – is nonetheless a likely possibility as vehicle systems rely more heavily on sophisticated computer-driven electronics.ʼʼ

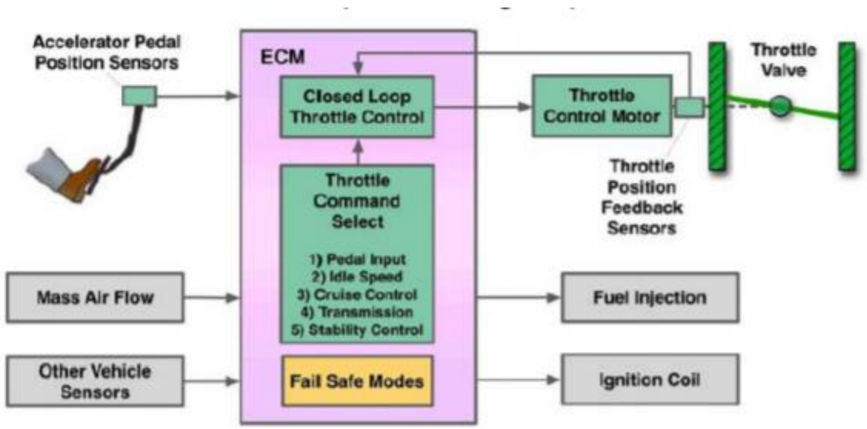
Toyota Sudden Unintended Acceleration

- Car’s electronics cause the throttle to go wide open, making it impossible for the driver to return the car to idle if it remains in gear

- severely limits the ability of the brakes to bring the vehicle under control -- leaving the unsuspecting driver at the mercy of a runaway car.

- Thousands of people, including drivers, passengers, and innocent bystanders, have been killed or seriously injured in sudden acceleration accidents.

Electronic Trottle Control System - ETCS



Source: P. Koopman. (2014) A case Study of Toyota Unintended Acceleration and Software Safety.

https://users.ece.cmu.edu/~koopman/toyota/koopman-09-18-2014_toyota_slides.pdf

Toyota Sudden Unintended Acceleration

“Whatever the root cause or causes of unintended acceleration, Toyota has been aware, for at least two years, that drivers who found themselves in a runaway vehicle **had no idea how to stop it**.

Naturally, the first reaction was to stand on the brakes, but **repeated application of the vacuum brake system actually rendered it useless**. The lack of a proper failsafe was identified in the Closing Resume of Engineering Analysis”

*“**Stopping the vehicle** while the throttle is fully open requires significant pedal force, which some operators did not, or were unable to, apply for the required duration.*

*Continued driving in this condition results in **overheated brakes**, which further diminishes the braking effectiveness.*

Some operators attempted to turn the vehicle off by depressing the engine control button, however they were unaware the button had to be depressed for three seconds to stop the engine when the vehicle is in motion; this functionality was not explained adequately in the owner's manual.’’

Sean Kane, Ellen Liberman, Tony Di Viesti, Felix Click. Safety Toyota Sudden UnintendedAcceleration, Safety Research & Strategies, Inc., 2010, http://www.safetyresearch.net/Library/ToyotaSUA020510FINAL.pdf

Toyota Sudden Unintended Acceleration

Regardless of the causes of sudden unintended acceleration in Toyota and Lexus vehicles, the automaker’s first step should be measures to protect the public.

⬇

The implementation of a brake-to-idle feature across all model lines and years may be a significant step in that direction. With this feature, the signal to brake would take precedence – even if the throttle were fully open. The brake override allows drivers to regain control of a runaway vehicle.