University of Victoria Engineering

ENGR 110 / 112 – Design I

Failure

Failure in Engineering

Instructor: Dr. Flavio Firmani

University of Victoria Engineering

Failure in Engineering Design

Historically, engineering has been a main contributor for increase in life expectancy, improvement of health conditions, and increase in mobility and productivity, among others.

Advancements in technologies have made possible to develop efficient systems of transportation, housing and shelter, agricultural production, sanitation and waste management, essential medical devices, medical care, etc.

Nonetheless, failure in products exist, and as engineers we try to mitigate and learn about designs that fail.

EGBC Code of Ethics: *Hold paramount the safety, health, and welfare of the public, including the protection of the environment and the promotion of health and safety in the workplace.*

University of Victoria Engineering

Failure in Engineering Design

Product Failure:

Reliability: Products have a life cycle, and it is common that a product may fail after a period of time. Recommendations based on statistical data are made to replace parts of a product.

Quality Control: In order to ensure the quality of their products, companies test units and determine if they remain within the specifications for the final product.

Testing can be done at different stages of the manufacturing process to determine any needs for corrective actions in the manufacturing process. Statistical analysis is employed to check if there is any significant variation.

Product Recalls: Companies request to return a product when there is evidence that a faulty product can endanger the consumer.

University of Victoria Engineering

Failure in Engineering Design

Failure in Design:

Failure in design can originate at any stage of the design process

Problem Definition: A common design failure is to design a system that does not solve the needs of the client or consumer. In general, these designs never hit the market.

Conceptualization: history shows that especially when stepping outside an existing design space, failures occur.

Detailed Design: A number of incidents have occurred due to improper calculations or incorrect conversion of units.

University of Victoria Engineering

Failure in Engineering Design

It is expected that engineers follow the design process and apply the best technical knowledge and analytic skills when carrying out engineering design.

Notwithstanding the many successes of engineered systems, there have been numerous failures that can be hard to diagnose, and impact or even injure/kill many people. Failures can also occur as systems become increasingly complex, or where management/regulation frameworks break down or are no longer fit in the modern area.

The introduction of new materials and technologies have historically involved hard lessons learned from design failures owing to misunderstood or un-identified physical phenomena.

University of Victoria Engineering

Failure in Engineering Design

Disasters, especially in modern engineering systems, are rarely the result of a single mistake. Design decisions, as-built errors or changes and operational circumstances all typically contribute.

Most modern engineered systems involve embedded software/hardware. The careful design and testing of those control systems, including human-computer interaction effects, is critical to avoid design failure.

Engineers have a responsibility to ensure their work is thoroughly checked, and products/systems produced based on their designs is physically (or through software) implemented according to the design specifications.

Always check unit conversion on any calculations you ever do.

University of Victoria Engineering

Therac - 25

Therac – 25 was a computer-controlled radiation therapy machine produced by Atomic Energy of Canada Limited (AECL) .

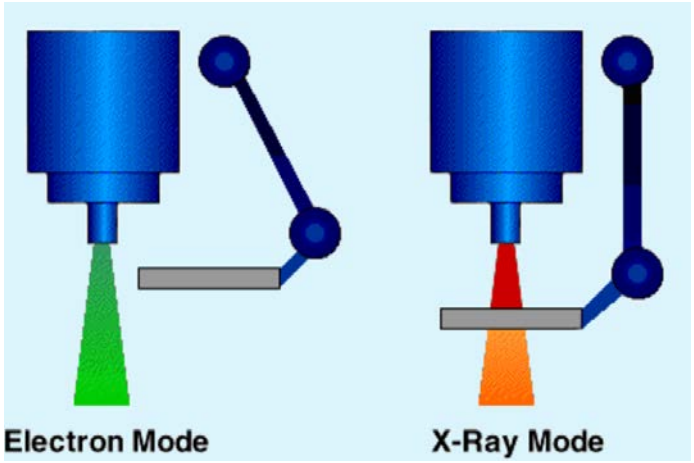
Six people died due to a radiation overdose caused by a “bug” that controlled the software of the machine

University of Victoria Engineering

Therac - 25

Therac-25 reused code from earlier machines, and some hardware features were replaced by software features.

Machines with dual mode, electron (low radiation – direct application) and X-ray (high radiation with metal plate), position the required equipment with a turntable prior to triggering the dose of radiation. Older machines checked the mode with hardware, Therac-25 checked this with software.



Therac - 25

When the machine was set to X-ray mode, it took about 10s for the machine to setup; however, if the operator suddenly changed the mode to electron mode fast enough within those 10s, the turntable would not have time to switch to the correct position.

Checking the mode implied whether the cursor was in the cmd prompt.

As a consequence, patients were exposed to radiation that was 100 times more than the treatment.

```
Datent:
  if mode/energy specified then
    begin
      calculate table index
      repeat
        fetch parameter
        output parameter
        point to next parameter
      until all parameters set
      call Magnet
      if mode/energy changed then return
    end
  if data entry is complete then set Tphase to 3
  if data entry is not complete then
    if reset command entered then set Tphase to 0
  return

Magnet:
  Set bending magnet flag
  repeat
    Set next magnet
    Call Ptime
    if mode/energy has changed, then exit
  until all magnets are set
  return

Ptime:
  repeat
    if bending magnet flag is set then
      if editing taking place then
        if mode/energy has changed then exit
  until hysteresis delay has expired
  Clear bending magnet flag
  return
```

University of Victoria Engineering

Lithium-Ion Batteries

Lithium-Ion batteries are the leading technology of rechargeable batteries in mobile phones and laptops.

They are light, charge lasts longer, greater discharge cycles, relatively inexpensive, high energy density (stored energy relative to its weight), but there have been incidents of cellphones and laptops overheating and catching fire.

Samsung was forced to recall Galaxy Note 7 in 2016 costing $5.3bn USD.

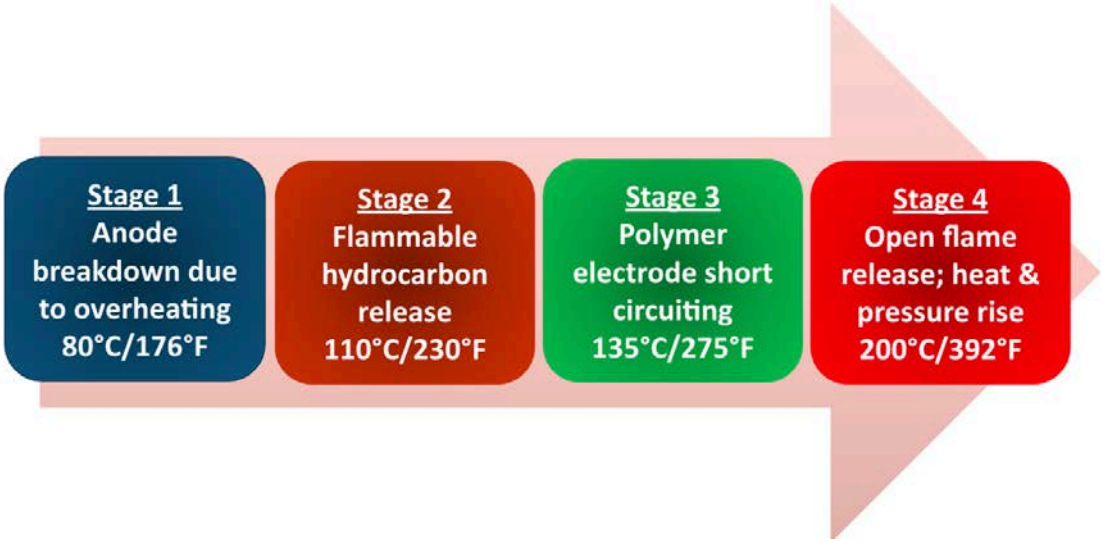
University of Victoria Engineering

Lithium-Ion Batteries

Lithium-Ion batteries contain a flammable electrolyte

If a cell generates more heat than can be dissipated, and heats above 80 °C, decomposition of the electrolyte layer takes place.

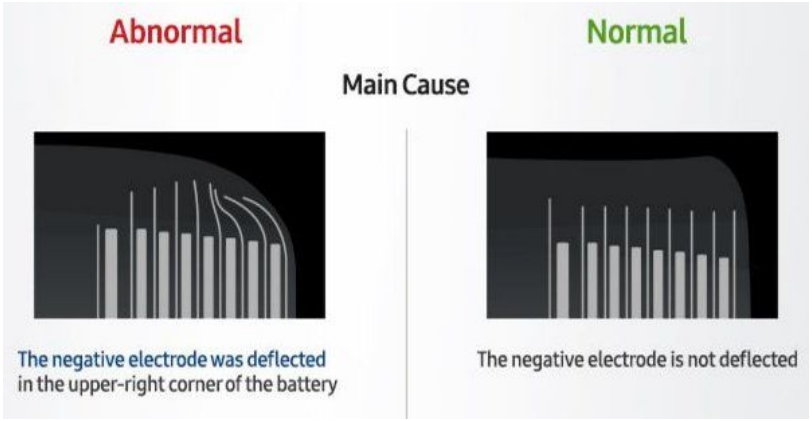
Cell enters the thermal runaway regime between 130 and 220 °C.



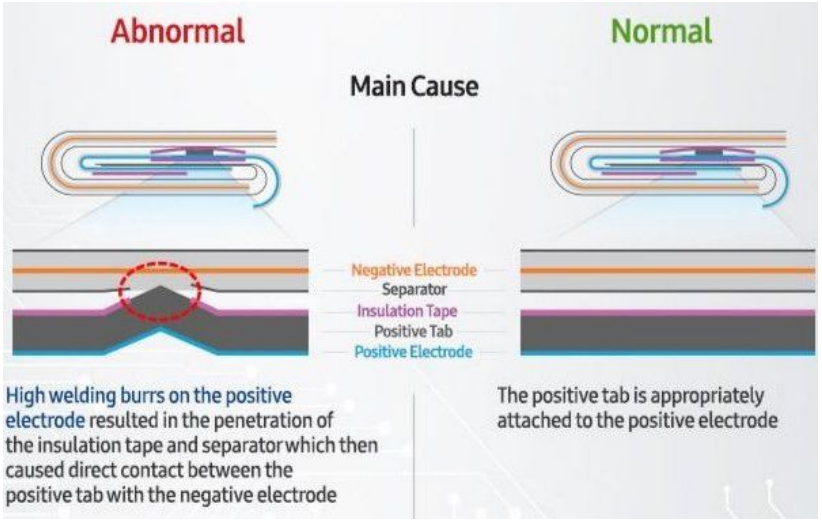
Galaxy Note 7

The main reason of the thermal runaway was cause by poor design.

Samsung tried to reduced the size of the phone at the expense of the battery safety. Poor design to safely accommodate the electrodes and insufficient insulation material were the major problems.



When batteries charge, chemical processes causes the battery to mechanically swell. About 10% of extra space is required but the battery on th Note 7 entirely filled this pocket.



Samsung confirms battery faults as cause of Note 7 fires - BBC News

University of Victoria Engineering

Canadarm1

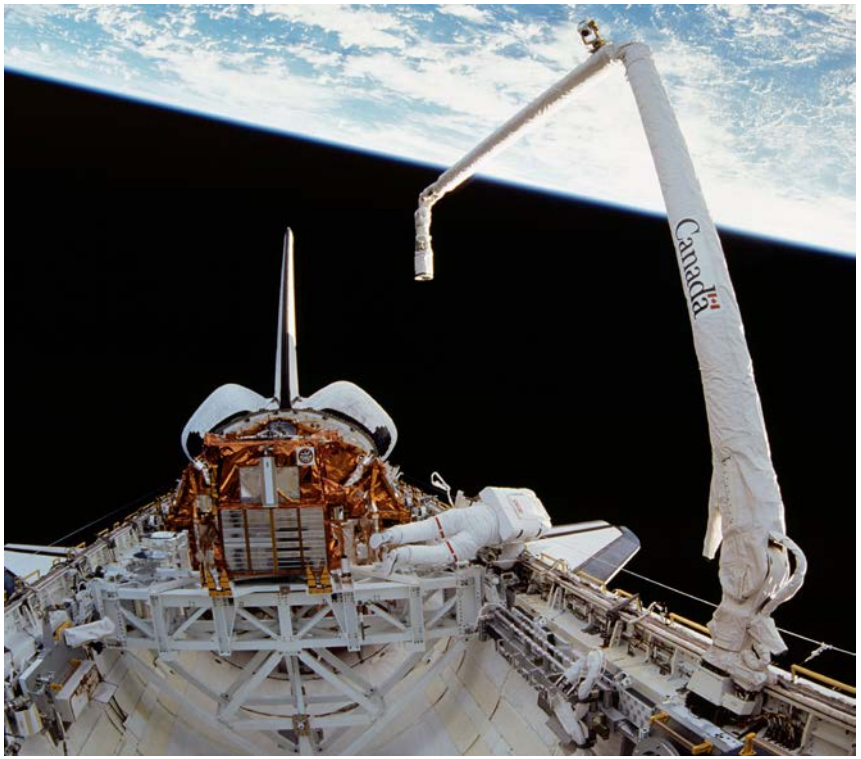
Canadarm1 could have caused one of the greatest engineering catastrophes in history.

This 6-DOF arm was used along the space shuttle orbiters.

The ISS uses solar panels to power the station. Since power is limited, devices take turns to operate.

Cadadarm1 was connected at both ends for several hours and exposed to large temperature changes.

When released, the thermal shock almost hit the ISS.

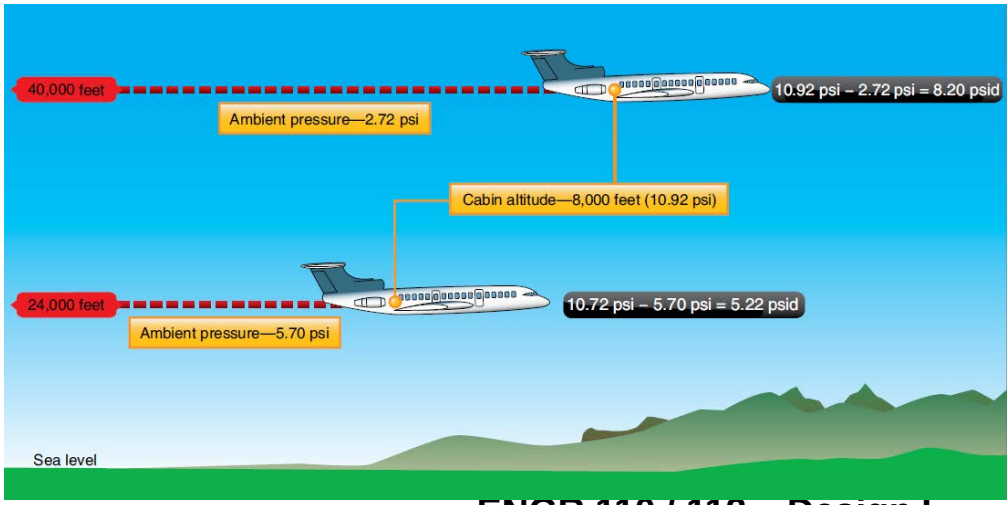


Havilland Comet

The Havilland Comet revolutionized aviation, as it was the first jet used for commercial flights.

The Comet flew at 40,000 ft, where there is thin air and less drag, and therefore reducing considerably fuel consumption, compared to the other airplanes flying at 10,000 ft.

At this altitude, the plane had to be pressurized, 18 KPa at 40k ft compared to 70 KPa at 10k ft.



University of Victoria Engineering

Havilland Comet

After a few incidents where pilots were blamed, two fatal incidents in the Mediterranean where the planes exploded in midair led to an investigation.

The reason of the explosions was the continuous cycles of pressurization and depressurization, which caused fatigue to the fuselage (expansion and contraction of metal).

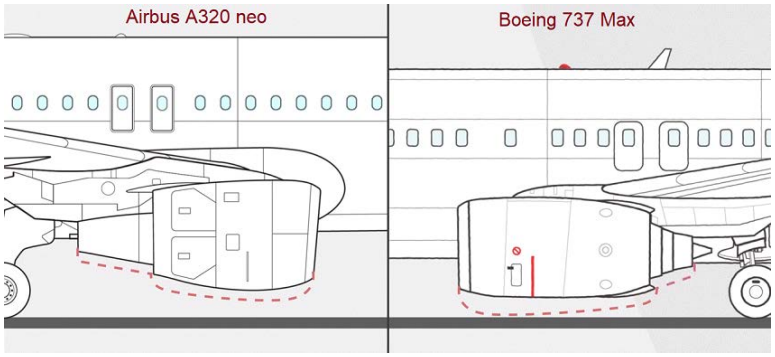
University of Victoria Engineering

Boeing 737 MAX

In 2010, Airbus was coming out with an updated version of the A320 family that it called the A320neo, with “neo” meaning “new engine option”. The new engines were going to be more fuel-efficient, with a larger diameter than previous A320 engines. The A320 competes with Boeing’s 737 family of airplanes.

***Economic problem*:** 737 engines used too much fuel. To stay competitive, Boeing had to install new, more efficient engines with bigger diameter fans.

Airframe problem: Boeing wanted to reuse the 737 airframe but needed more ground clearance with bigger engines. The 737 design can't be practically modified to have taller main landing gear. The solution was to mount the engine nacelle higher and more forward on the plane.

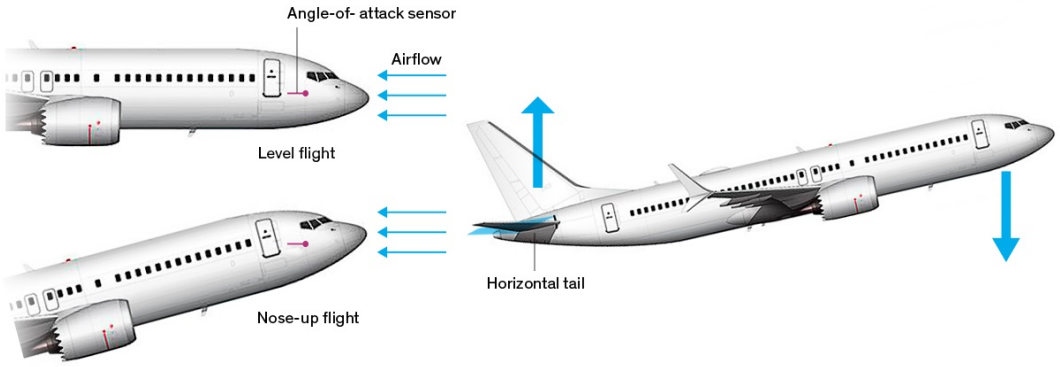


University of Victoria Engineering

Boeing 737 MAX

Aerodynamic problem: Moving the engine nacelle changed the aerodynamics of the plane, such that the plane **did not handle properly at a high angles-of-attack** to be certifiable. Boeing created the Maneuvering Characteristics Augmentation System (MCAS) to electronically correct for the aircraft's handling deficiencies.

Systems engineering problem: Boeing wanted the simplest possible fix that fit their existing systems architecture, so that it required minimal engineering rework, and minimal new training for pilots and maintenance crews. The easiest way to do this was to add some features to the existing Elevator Feel Shift system (EFS). Like the EFS, the MCAS relies on **non-redundant** sensors to decide how much trim to add. However, unlike the EFS system, MCAS can make **big nose down trim changes**.



University of Victoria Engineering

Boeing 737 MAX

On both ill-fated flights (Indonesia and Ethiopia), there was a:

- ***Sensor problem:*** The angle-of-attack vane (airflow sensor) on the 737 MAX appears to not be very reliable and gave wildly wrong readings.
- ***Maintenance practices problem:*** The previous crew had experienced the same problem with the angle-of attack vane and did not record the problem in the maintenance logbook.
- ***Pilot training problem:*** Pilots were never told about the MCAS, and even after an emergency Airworthiness Directive was issued after the first accident, no one had done simulation training on this failure. Pilots were inexperienced, they could have run stabilizer trim runaway checklists to correct the problem.
- ***Economic problem:*** Boeing sells an option package that includes two additional sensors: an **extra angle-of-attack vane** and an **angle-of-attack disagree light**, which lets pilots know that this problem was happening. Both 737 MAX airplanes that crashed were delivered without this option. No 737 MAX with this option has ever crashed.

University of Victoria Engineering

Hyatt Regency Hotel

A number of fatal design failures have occurred in the area of civil engineering, for example the Quebec Bridge collapsed twice during construction in 1907 (75 death) and 1916 (13 death).

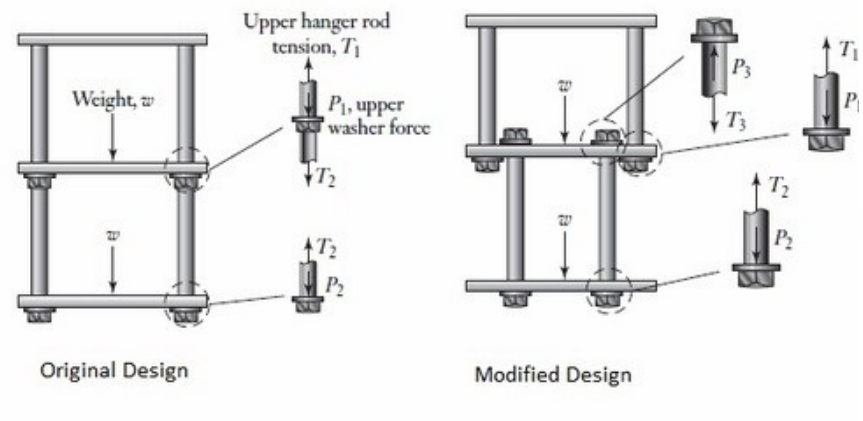
Another example, two of the vertical walkways of the Hyatt Regency Kansas City collapsed directly onto a partying crowd in the hotel lobby in 1981. The tragic incident took lives of 114 people and injured 216 people.

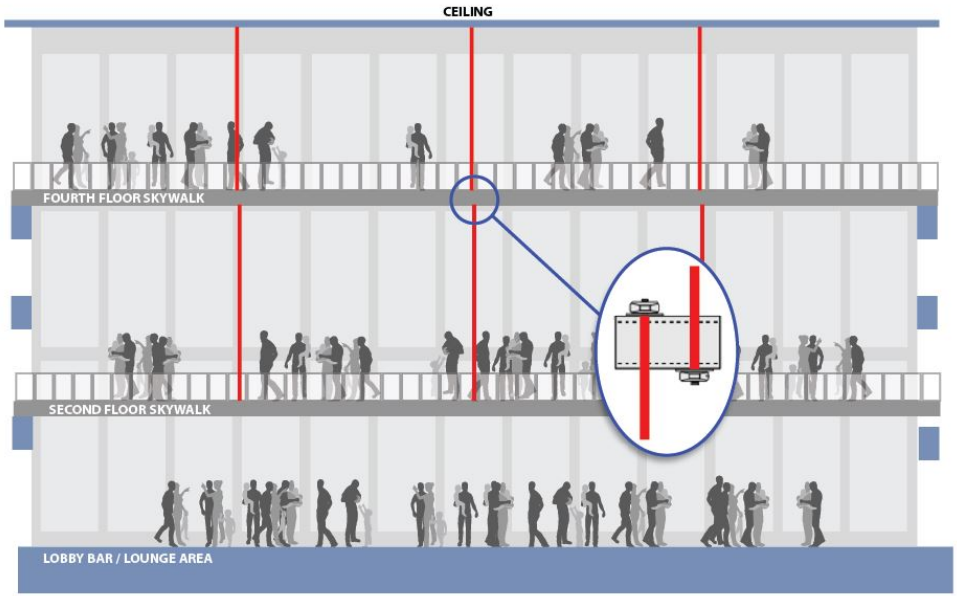
University of Victoria Engineering

Hyatt Regency Hotel

The original design was changed, as the fabricator noted that having nuts and washers in the middle of the hanger rod would require a full length of thread between the second and fourth floor walkways.

Thus, a new design was proposed, by splitting the hanger rods in two halves. This subtle change became catastrophic.





University of Victoria Engineering

Measurement/Unit Mistakes

Simple measurement mistakes, such as units, can be very costly!

The **Laufenburg Bridge** connects Switzerland and Germany. Both countries built half of the bridge relative to the sea level. Germany used the North Sea and Switzerland the Mediterranean Sea. By the time the two half-bridges met, there was a 54 cm difference (2003).

The **Great Kersten Blunder**. Software controlling the Vigor space probe, on course for Venus, used 24.5 instead of 25.4 to convert millimetres to inches. The error meant that the probe missed Venus completely, and $2 billion worth of technology was lost (1998).

Tokyo Disneyland's Space Mountain Derailment. The Space mountain roller coaster ride broke an axle during the middle of the ride causing one of the two roller coaster cars to derail (2003). The reason: an incorrect conversion from Imperial to SI units.

University of Victoria Engineering

Measurement/Unit Mistakes

NASA's Mars Climate Orbiter programming teams in Europe and the USA used two different measurement systems to calculate the trajectory of the spacecraft. The probe consequently entered the Martian atmosphere at the wrong angle, and promptly disintegrated (1999).

The **'Gimli Glider'** is referred to an Air Canada flight incident from Montreal to Edmonton (July 1983). The aircraft was refueled in Montreal using an incorrect conversion.

22,300 kg (required) − 13,597 lb (in tanks) = 8,703 kg (refuel)

When the plane ran out of fuel mid-flight, the pilot had to make an emergency 'gliding' landing at Gimli (Manitoba) Canadian Air Force Base.

University of Victoria Engineering

Recommended TED Talk Videos

- Celebrating Failure - Astro Teller
https://www.ted.com/talks/astro_teller_the_unexpected_benefit_of_celebrating_failure?language=en

- Start-up Companies - Bill Gross
https://www.ted.com/talks/bill_gross_the_single_biggest_reason_why_startups_succeed