LESSONS TO BE LEARNT

July 2021

engineering new zealand
te ao rangahau

CONTENTS

1: INTRODUCTION

This webinar looks at examples of engineering disasters caused by people failing to contemplate the possibility that they may be wrong through ‘hubris’ - an extreme and unreasonable feeling of pride and confidence.

For example, going beyond what current technology can do (such as with bridges failures) or when there is a Swiss cheese situation (where all the minor mistakes made by people added up to a disaster).

Lessons to be learnt from these examples can be applied to our own practice and professional development.

2: WHAT HAPPENED

The following examples of engineering disasters are underpinned by hubris. For example, thinking ‘I've got it right’, ‘I know what I'm doing’, ‘Go away and don't tell me anything else.’

EXAMPLE: THE ENIGMA MACHINE (1939-1945)

The Enigma machine was a coding machine developed by the Germans in the 1930s and used during World War Two to ensure secure communication.

The Germans believed it couldn't be cracked. It had multiple rotors, which worked together to transpose letters, offering 3 x 10^{114} possible letter combinations. They assumed there was no conceivable method you could decode what went into in or what was coming out of it.

What happened?

Britain put together a team dedicated to decoding the enigma machine, who developed a mechanical device called the Bombe. It was full of relays and wires spinning which worked to decode a message by trial and error. It kept going through thousands of combinations until it found the combination that worked to break the code.

Britain also developed another machine to work faster than the Bombe. It was the world's first electronic computer, called Colossus, and it likely shortened the Second World War by several years.

How was hubris displayed?

The Germans were convinced their code couldn't be broken. For example, they changed their naval codes and for a year and the British didn't know where the German submarines were. Then suddenly the British broke the code, and German submarine losses skyrocketed. Because of their belief in Enigma, as well as the success of British counter-intelligence, the Germans didn’t think "Maybe they've broken our code."

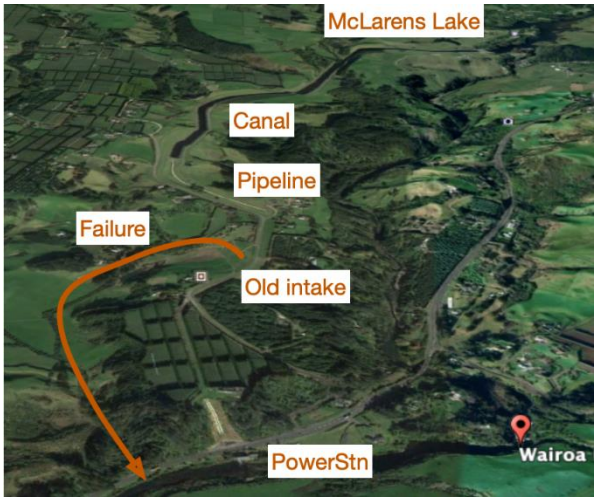
EXAMPLE: RAUHIHI HYDRO SCHEME (1981)

Ruahihi is a New Zealand hydro scheme that failed in 1981. It was designed 10 to 15 years earlier by Lloyd Mandeno and consisted of an existing lake (McLarens Lake), a 3350m concrete-lined canal through volcanic debris to a low-pressure conduit, and then through penstocks (pipes) down to the power station at the river, approximately 80m ahead.

What happened?

Although initially designed by Lloyd Mandeno, after his death it was re-designed, including changing the original concrete-lined canal specification to an earth-lined one.

The scheme failed the day after it opened in 1981 in one go. The canal leaked, with the water eroding the ground and a large hole developed in the lining. It kept going up the canal until it all washed down to the intake structure in the dam, and the side of the canal collapsed in one go. Fortunately, there were no injuries or lives lost, but it was an unimaginable mess.



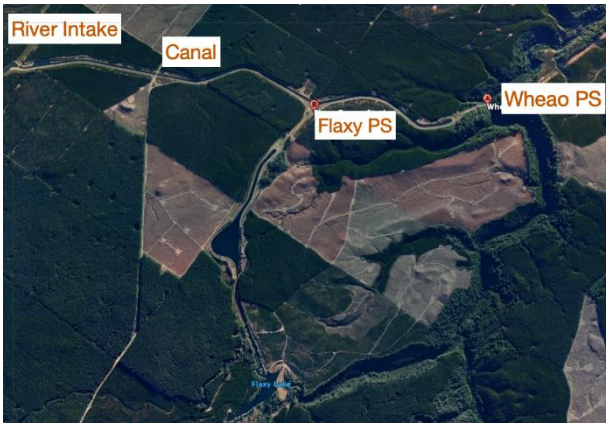
How was hubris displayed?

The investigation found a range of issues:

- There was a turnover of the specialists involved in the project and possibly a loss of institutional knowledge and expertise.
- There was not enough recognition of the nature of the environment, such as volcanic materials, in the planning, detailed investigation and design stages.
- Swapping out a concrete-lined canal for an earth-lined canal (brown ash) was not appropriate for the volcanic nature of the environment:
    - they didn't foresee that the brown ash would dry out and crack
    - they should have known that the cracks would not re-seal when it was filled with water, and
    - they ignored advice on ground conditions
- When it became apparent (not long before it was commissioned) that water leaked out of the bottom of the escarpment the canal was built on, they put drainpipes in. This hid the problem, as they could no longer see where the water was coming from, but the leaking water continued to erode the ground
- When water started leaking out of the bottom of the escarpment, they delayed shutting down the canal until the Monday after the official opening.

EXAMPLE: WHEAO SCHEME (1982)

The Wheao scheme is another New Zealand hydro scheme where the canal failed in 1982. The scheme consisted of a stem with a river intake, a long canal through volcanic country (volcanic ash deposits) down to the top of a quite steep escarpment with the powerhouse about 125m below.

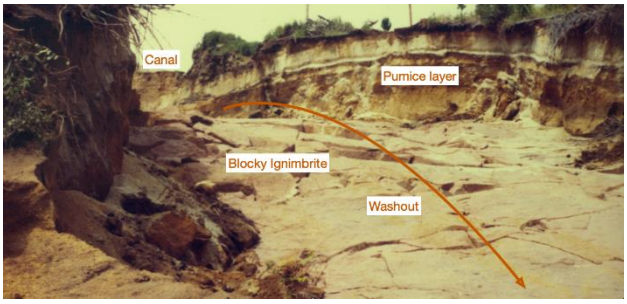


What happened?

The scheme failed after an inadequate leak repair opened, with water leaking halfway down the escarpment.

In the repair, the intake was moved upstream, because the geological conditions at the site of the old intake were poor. The turbines and generators were also repaired, and money was spent on aspects unrelated to the failure.

Moving the intake further upstream was a mistake. The new intake site was sitting on fractured ignimbrite (which was known to be problematic) and other volcanic deposits, including a pumice layer. Water forced its way under the concrete lining, split open the fractured ignimbrite and washed out the pumice layer. A significant rupture of the canal occurred, bypassing the intake, and flooding the power station.



How was hubris displayed?

The civil engineers (designers) were a Hamilton-based company with an office in Rotorua (supervisors), with another company brought in for the mechanical and electrical side. The civil engineers:

- designed the scheme in Hamilton and supervised it from Rotorua, which proved problematic as the Hamilton office mistakenly thought the area in front of the intake had been grouted
- failed to communicate, such as providing the specification for turbines
- did not update information needed by electrical and mechanical engineers
- ignored lessons from the Ruahihi disaster the year before, even when questions were raised by other engineers.

After the repair failed, the scheme was repaired again (the turbines, generators, and civil works) to the required standard and it's now been running for forty years.

EXAMPLE: COLUMBIA SPACE SHUTTLE DISASTER (2003)

The Columbia Space Shuttle broke apart in 2003 when it came into land, killing all seven crew members. It was the second of two space shuttle disasters in the US space program. The first was the Challenger in 1986 which broke up soon after take-off.

What happened?

In the Columbia incident, heat-resistant tiles had dislodged off the wing. This meant that when the shuttle came in to land, the heat got through, destroyed the aluminium underneath and caused the space shuttle to disintegrate.

How was hubris displayed?

According to the official report[1], NASA took great pride in its history and its 'can do' attitude. It saw itself as 'the perfect place' following the success of its Apollo programme and had a lot of self-confidence about possessing 'unique knowledge' on how safely to launch people into space (and didn't listen to criticism from the outside easily). It was not a 'learning organisation' and suffered from "flawed decision making, self-deception, introversion and a diminished curiosity about the world outside the perfect place".

The shuttle was developed as a re-usable space craft, but it was expected to have significant testing, upgrades, and replacement. However, multiple budget cuts at NASA meant that the programme didn't occur as anticipated.

- When a new technically ignorant management took over after the Challenger launch failure, they insisted the Columbia should fly on a certain date. There was an opportunity to inspect the tiles, which wasn't taken up.
- Engineers were under a lot of pressure from the new management (who did not have engineering expertise), who took over after the first shuttle disaster, to keep the shuttle flying. Management didn't understand the engineers and were not prepared to listen to them.
- Although the space shuttle was supposed to take off, fly and land over and over like an airliner, it didn't take the same rigorous design, develop and testing approach as a new airliner (which would have flown hundreds and hundreds of times and had modifications made until proven to be reliable and safe). Only then would it have been put into commercial service. Every time the shuttle landed, a lot of maintenance work had to be completed, so it never flew as often as they predicted.
- The shuttle tiles were often damaged by dislodged tank insulation. The big fuel tank (with liquid nitrogen) was covered with insulation which used to shed in big pieces. Everybody assumed that it was soft insulation, and it wouldn't do any harm.
- In the Columbia, a large piece of insulation came off at take-off and managers limited the inspection of the tiles in space (reasoning the crew would not have been able to fix the problem anyway).

[1] https://web.archive.org/web/20060105050618/http://caib.nasa.gov/

EXAMPLE: 737 MAX DISASTER (2018, 2019)

Two virtually new Boeing 737 MAXs crashed just over four months apart in 2018 and 2019.

What happened?

The 737 MAX had a problem with its control gear. Each crash was caused by a single malfunctioning sensor which left the pilots with a flight control system that ultimately forced their jet into a nosedive.

How was hubris displayed?

A major airline ordered a large number of planes from Boeing's competition, Airbus, and Boeing wanted to be able to offer the same deal.

The Airbus A320 promised larger more efficient engines and increased fuel efficiency. It could do this because it was:

- a relatively modern plane
- high enough off the ground to fit a larger new engine underneath the wing
- almost exactly the same plane for the pilot to fly as the earlier model.

Boeing then promised a 737 MAX with efficient engines and with no need to re-train pilots. But there were issues with the Boeing 737 MAX from the start as:

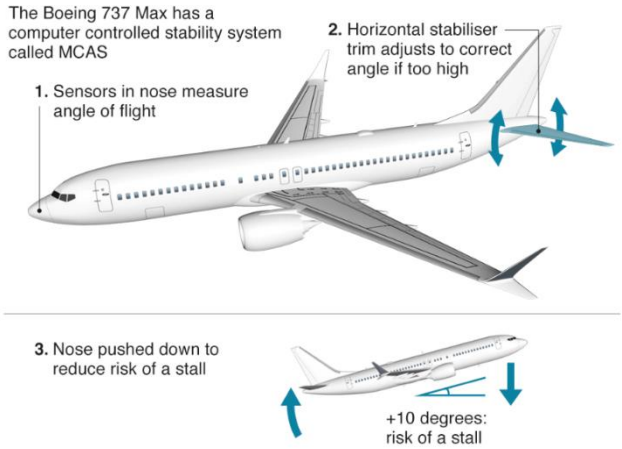
- it was over 50 years old
- larger engines couldn't fit under the wings, so they had to be placed up and forward
- testing revealed the heavier engines and the forward placement location of the engines on the created new and unsafe flight characteristics. Basically, when you opened the throttle, the nose went up and there was a risk the aircraft would stall and crash.

Note how low to the ground the original 737 is, making it impossible to fit larger engines under.

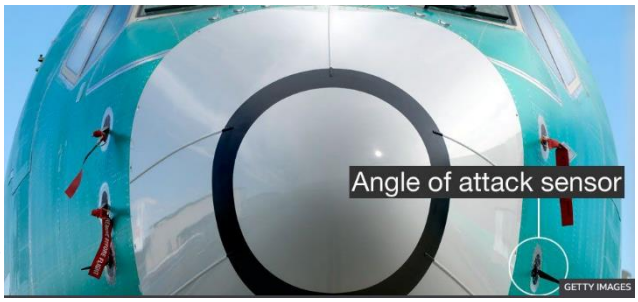
Note the engine location of the 737 MAX with the big engines placed up and forward, to be able to fit them in.

Rather than accept the company had pushed the original design of the 737 far past its limit, Boeing came up with a software solution. The engineers devised the Manoeuvring Characteristics Augmentation System to 'solve' the problem. To avoid getting involved in re-certification and re-training it relied on one of a pair of sensors to detect an incipient stall. This meant if a single sensor failed, the plane could crash.

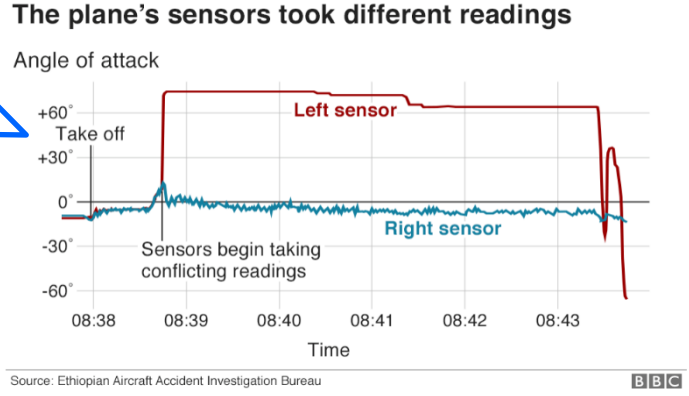
The system was kept secret from the pilots. Engineers within Boeing complained but were ignored.



The system relied on only one of a pair of sensors to detect an incipient stall. And if this sensor failed, the plane could crash.

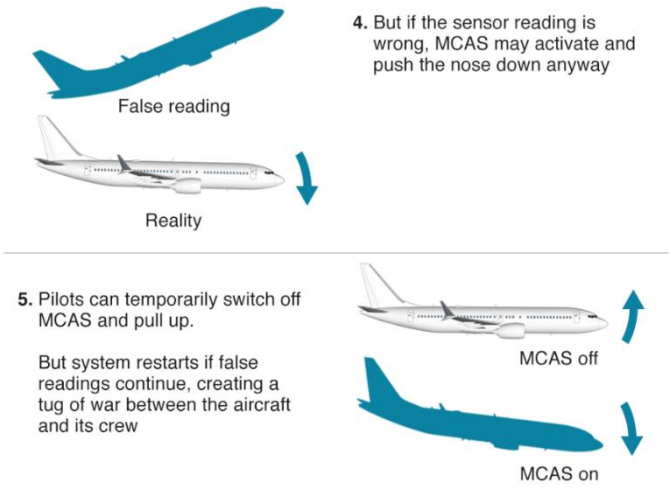


Each sensor took different readings.



Even if a sensor took a false reading (if the plane was flying normally) it pushed the stick forward and forced the nose down.

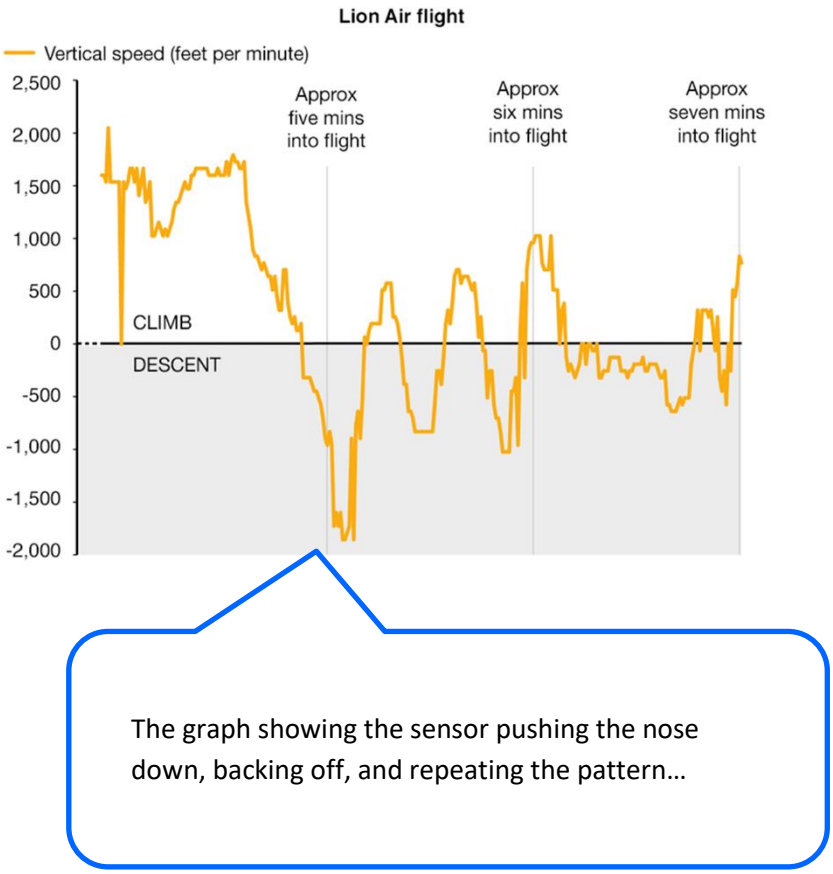
Then it would back off, so the pilots would suddenly have control again. Five seconds later it would cut in again, pushing the nose down. And so it goes on until, in the end, the plane crashes.



The report into the MAX crashes said they were not the result of a single failure, technical mistake or mismanaged event. Rather they were *"…The horrific culmination of a series of faulty technical assumptions by Boeing's engineers, a lack of transparency on part of Boeing's management, and grossly insufficient oversight by the FAA."*[2]

The report painted Boeing as a business under intense financial pressure – first to get the 737 MAX in the air, and then to maximise production at all costs. The desire to meet these goals, it said, had jeopardised the safety of the flying public.

Hubris.



The graph showing the sensor pushing the nose down, backing off, and repeating the pattern…

[2] https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf

3: LESSONS TO BE LEARNT

The key lesson from these engineering disasters is to never ignore the possibility that we are wrong, and to challenge what we are told and our own assumptions. Science is never settled.

There are generally reasons why engineers make decisions, and assume they are right, or what they are being told is correct.

- At Wheao, the engineering decisions resulted in the failure of the scheme.
- At Ruahihi, an earth-lined canal was used instead of a concrete-lined canal to save money, and the scheme had to be repaired.
- The Columbia space shuttle disaster highlighted our ethical issues and obligation to consider human lives.
- The 737 MAX airplane wasn't about cost, but about Boeing trying to win an order from a major airline, using a plane that wasn't suited, and using software to overcome bad design and keep a plane in the air.

4: IMPLICATIONS FOR PRACTICE

Never assume you are right or what you're being told is correct, even if it comes from a more senior person or a reputable source.

Reflect and question ideas and solutions as to whether they are right. It is our duty to tell others (including colleagues, clients, and the public) what they **need** to know, not what not we think they want to hear, and to ensure that this concern is accepted and acted on.

If needed, try a range of ways to get around organisational hubris: communication, peer review, and being realistic about what you can achieve in the required timeframe.

COMMUNICATION

Sharing information and communicating is good protection against hubris.

- Have open and frank dialogue. Discuss and explore better ways of doing things together.
- Exchange information transparently when you are working together. Don’t assume one group doesn't need to know anything.
- Get to know everybody and their expertise and build confidence in them.
- Some ideas for communicating effectively are:
    - email – copy everyone in to emails
    - get together face to face regularly in the large team to discuss everything, and
    - pick up the phone and have an open conversation.

Learn to tell people (including non-engineers) what they need to know, not what they necessarily ant to hear. It takes skill, but you've got to do it. Soft skills and communication are a vital, but often overlooked, part of engineering

- You've got to speak in language that they understand, not engineer's language.
- Use plain English and don't lose them in jargon or by going into too much detail.
- Work out what the key points are and make sure they come across. Just one or two single issues. For example, to get across that there is a potential for danger and to convince them that you know what you're talking about.

PEER REVIEW

Another key protection against hubris is peer review.

- Make sure you have good design in the first place (don't use peer review for a back up to failure of design.
- Get the design peer reviewed thoroughly and independently by someone who understands the New Zealand environment and requirements, and is happy to give a frank, independent and honest review. For example, someone who:
    - understands our geology around volcanic materials
    - follows the New Zealand drawing style
    - validates or verifies software results (for example when the input data is faulty)
    - works in a fast-paced environment, where decisions are required quickly, and management require response times (but don't take shortcuts).

A QUESTIONING MINDSET

Bring a questioning mindset to your work. Don't believe something just because somebody says it's true, including computer-generated information. If computers are given the wrong data, they produce the wrong answer.

- Follow up small changes to ensure any consequences/output are addressed.
- Ask yourself 'Does this add up to common sense? Does it fit with my experience, or should I go and ask questions? Is this reasonable, because it doesn't look right to me?'

PROMOTE ENGINEERING

Emphasise the importance of good engineering at every possible opportunity. There's a lack of engineering input and a lack of understanding by decision-makers into how important engineering is.

BE PART OF OUR COMMUNITY OF PRACTICE

Engineering New Zealand community of practice supports engineers in many ways. For example:

- With the Engineering NZ Library of webinars (growing all the time) **https://www.youtube.com/playlist?list=PLfmb4aWklbWBQZbMBd9SVvQ7USyx4GF5d**
- Promotion of CROSS-AUS or similar in your discipline. Look at the Engineers Without Borders failures website **http://reports.ewb.ca/**
- Better understanding the Human Factors for both individuals and organisations.

- Understanding our own limitations and competence. For example, Improving QA.
- Ongoing upskilling and learning.
- Peer to peer reviews of our work.
- Owning our mistakes and sharing them to promote better learning and engineering outcomes.
- Helping create a 'JUST culture' in your workplace and technical and professional organisations. Engineering New Zealand is currently exploring resources for companies to use around how to implement it.
- Sharing information and mistakes. This includes re-visiting past failures so a new generation of engineers can learn the lessons and we can avoid 'memory fade'.

5: REFERENCES

Engineering NZ Library of webinars

- **https://www.youtube.com/playlist?list=PLfmb4aWklbWBQZbMBd9SVvQ7USyx4GF5d**

Engineers Without Borders failures website

- **http://reports.ewb.ca/**