BAKERRISK®

Identify | Evaluate | Solve

Digitalization – What could possibly go wrong?

Roger Stokes

EPSC

6 July 2021

Copyright BakerRisk. All rights reserved.

Overview

- Introduction
- Examples of New Technologies
- Some historic examples of problems with new technology
- Management of Change and Human Factors associated with New Technologies
- Testing the Barriers
- Conclusions
- Questions

Industrial Revolutions

1. 1760s – 1860s
   Spinning Jenny, steam engines, coal, iron, railways
2. 1870 – 1960s
   Oil & Gas, Electricity, internal combustion, steel, assembly lines, chemical processes
3. 1969- ?
   Electronics, Microprocessors, Telecom, Digitisation
4. 2000 - ?
   Internet, connected devices (IoT), intelligent systems, AR, AI, Digitalization

Benefits of Digitalization

- Machines, systems, data, devices and humans communicating with each other in ways that are continuously evolving.
- Intelligent Systems/ Artificial intelligence can do better than humans

- Benefits include:
  - Increased productivity
  - Higher efficiency
  - New Innovation
  - Improved safety

➢ Improve the quality of life for everyone on the planet

Potential Risks of Digitalization

- In industries where the consequences of failure are severe:
  - Could also introduce new and potentially unacceptable risks.
  - Potential negative interactions between new ways of doing things and our existing systems
  - Human interactions and performance factors that are not fully understood and assessed
- Multiple examples where technical progress has led to incidents:
  - Much has been learnt to avoid similar failures
- But with yet newer technologies from digitalization:
  - May introduce new failure modes and types that are difficult to foresee.
  - *You don't know what you don't know (the unknown unknowns)*

BAKERRISK®

Identify | Evaluate | Solve

Examples of New Technologies

www.BakerRisk.com

Copyright BakerRisk. All rights reserved.

Examples of New Technologies

- Wearable technology
  - Cameras, gas detectors, personnel locators, smart PPE
  - Supervisor and others can see
    - Where they are
    - What they are doing
    - How safe and healthy they are
  - Data fed back to the control room and analytics systems.
- Permits to work can be digitized
  - Automated prompts/ standard methods.
  - Everyone has access to them.
  - Ease of auditing
- Locations of maintenance work more clearly identified
  - Bar codes/ QR codes/ GPS/ Radio Frequency (RF) devices.

Examples of New Technologies - 2

- Process isolations can be made “live” on the DCS
  - Operators in the control room can see which manual valves are closed.
- Checklists for high-risk activities can be completed digitally.
  - Potentially greater control
  - Improved auditing
- Smart sensors and analytics
  - Faster and more reliable leak detection
  - Continuous monitoring – mechanical integrity
- Big Data / Artificial intelligence
- Process Simulators
  - Operators trained on systems that are off-line
  - Coupled with virtual reality systems, this can lead to faster and more effective training.
- Digital twins
- Any many more…

BAKERRISK®

Identify | Evaluate | Solve

Historic Examples of Problems with New Technology

Example 1 - Vehicle Automation

Austin 1300 GT, circa 1970 (Car and Classic, 2020)

Vehicle Automation

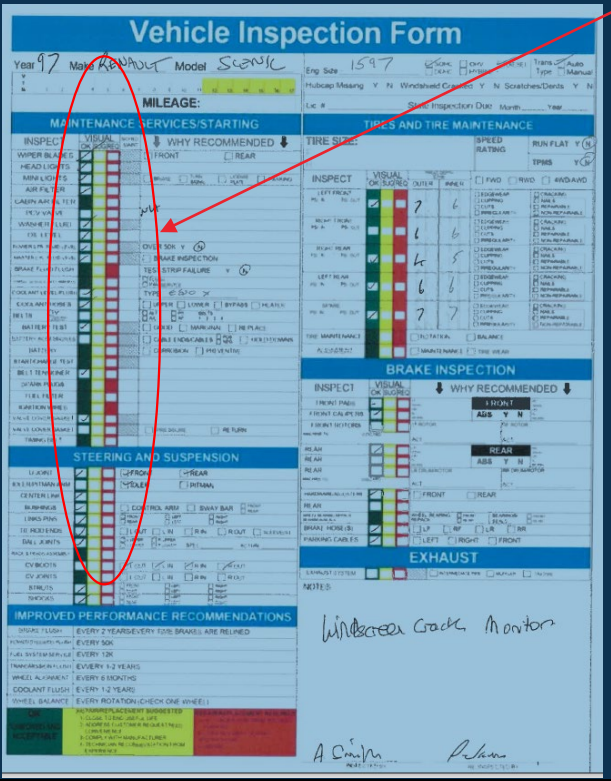
Driver Aid

*** Automatic Headlights ***

- Great for the forgetful !
- But two additional features …
  - Day running LED lights (on all the time)
  - They fitted an “off” switch”
- I still forget to turn them on
  - … and this is made more likely as I can see my day running lights in the reflection of the car in front!
- Net effect:
  - ➢ An increase in the likelihood of driving a considerable distance in the dark without full lights on.

Example 2 - Vehicle Checklist

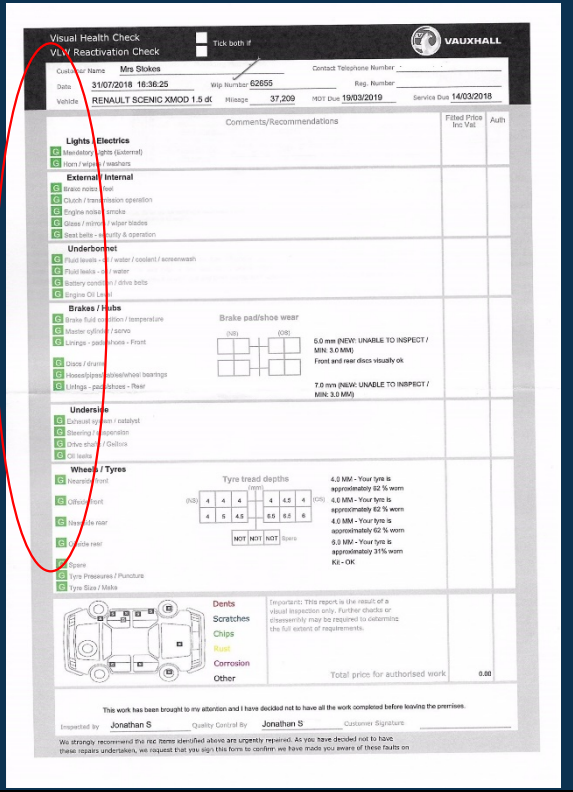
Manual Checklist



- Handwritten
- Individually ticked
- Slight oily
- Gives some reassurance work was actually done!

- Computer generated
- Printed in reception
- More comprehensive, retrievable and auditable records.
- Was there a “Tick All” option on the computer
- Was the work done?

Automated Checklist



Checklists in High Risk Industries - Aviation

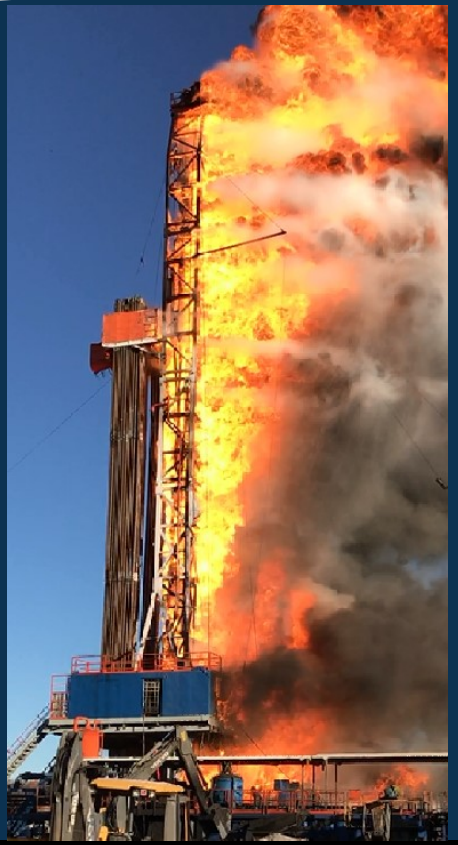
- *Making checklist procedures more automatic, either by asking crews to rely on system state as indicated by the checklist, rather than as indicated by the system itself, will discourage information gathering and may lead to dangerous operational errors **

- In the process industries, switching to a different type of checklist should involve a Management of Change procedure including a Human Factors analysis.

* *Mosier et al,1992*

Example 3 Blowout in Oklahoma Pryor Trust Well, January 22, 2018

- Not enough mud being pumped down an underbalanced well whilst drill pipe was removed (“Tripping”)
- Pressure in well > head of mud
- Blowout and fire killed five workers
- Many contributing factors
- **New electronic version of a trip sheet**
  - Included feature that automatically calculated the fluid balance in the well, rather than relying on a manual calculation
- Operator not trained in the use of the electronic trip sheet
- Drillers had also turned off the alarm system that was giving excessive nuisance alarms, masking more critical alarms



Blowout in Oklahoma – key issues

- New automated checklist system / inadequate training or understanding of the new system was a key causal factor with this incident.
- Management of Change system needs to ensure employees are involved in the details of procedural changes and are properly trained prior to start-up.
  - Would expect to be checked as part of a Pre-Start-up Safety Review (PSSR).

Example 4 – Boeing 737 Max

- Lion Air, Indonesia 28 Oct 2018 – 189 fatalities
- Ethiopian Airlines, 10 March 2019 – 157 fatalities

- Both attributed primarily to the repeated activation of an automated “Manoeuvring Characteristics Augmentation System” (MCAS) following an erroneous reading from an angle of attack sensor

- Many other factors in both cases

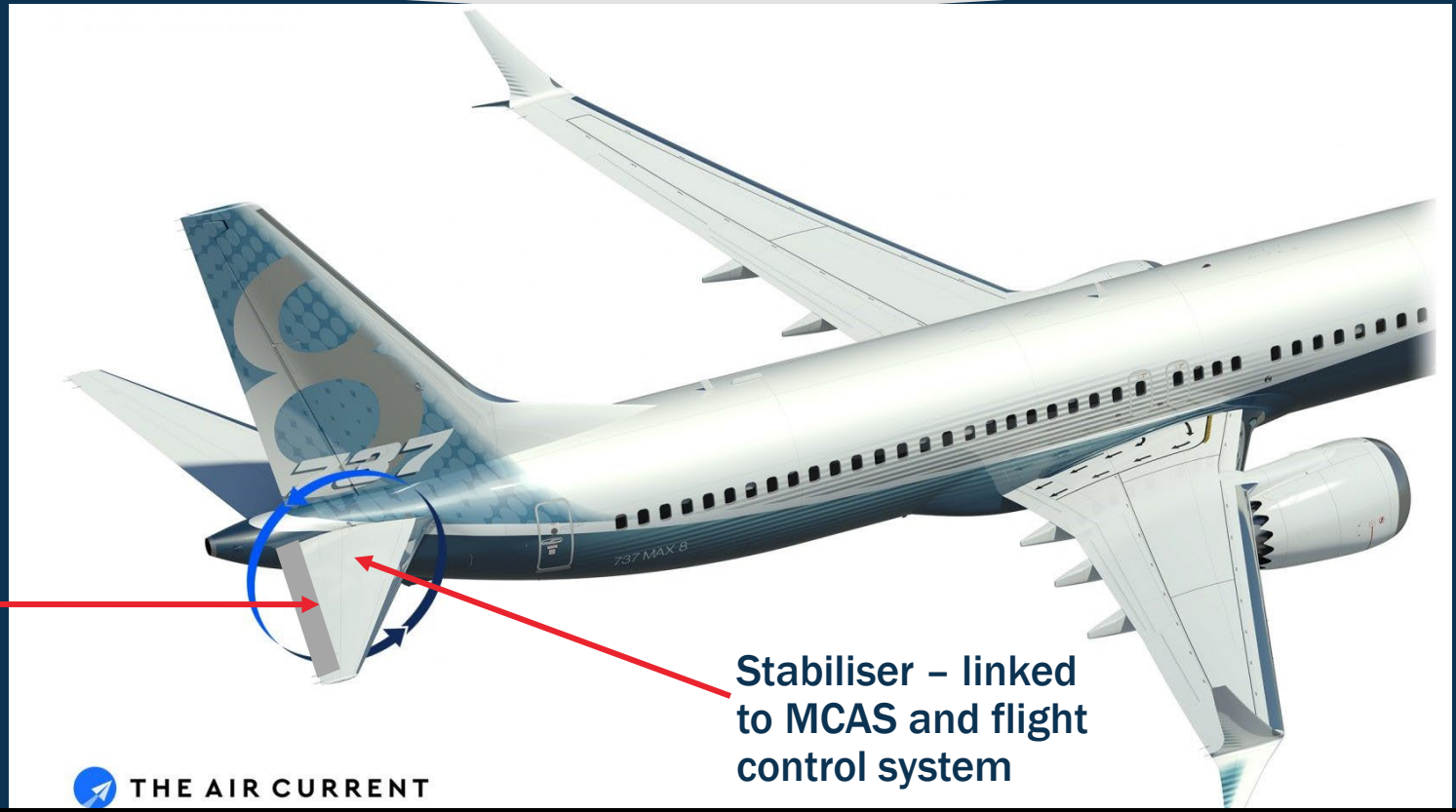
737 Max - History

- 1st Generation in service since 1968
  - Prior to the introduction of sophisticated electronic flight instrumentation systems
- Subsequent design iterations included
  - Addition of more sophisticated electronic systems
  - Basic flight control systems remained electro-mechanical and hydraulic
  - Not full “fly by wire” systems.
- 4th Generation, into service 2018
  - More efficient CFM engines, larger diameter, mounted forward
  - Resulted in a nose-up tendency under high power levels

737 Max - MCAS

- Maneuvering Characteristics Augmentation System
- To counter the nose-up tendency
- Activates automatically
  - If single angle-of-attack sensor goes beyond pre-set limit
- Prevented the Max from having different handling characteristics to that of its predecessors.
  - No change to aircraft “type” assessment
  - No simulator training for pilots (cheaper for operators)
- Its existence not included in Boeing’s Operations Manual
- Two AoA sensors fitted
  - But “disagree alert” for the two sensors not functioning on many 737 Max aircraft

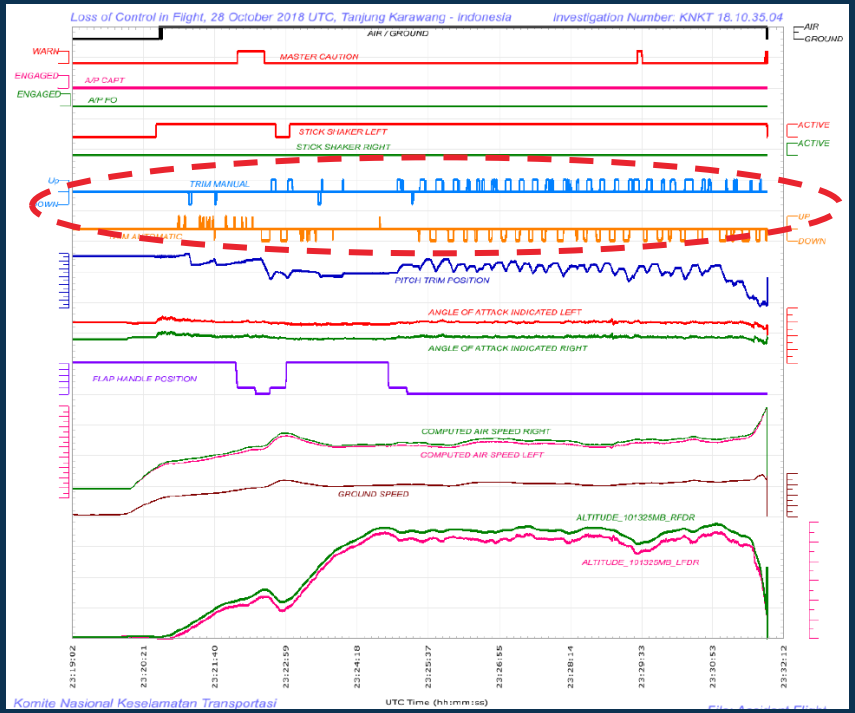
737 Max - MCAS

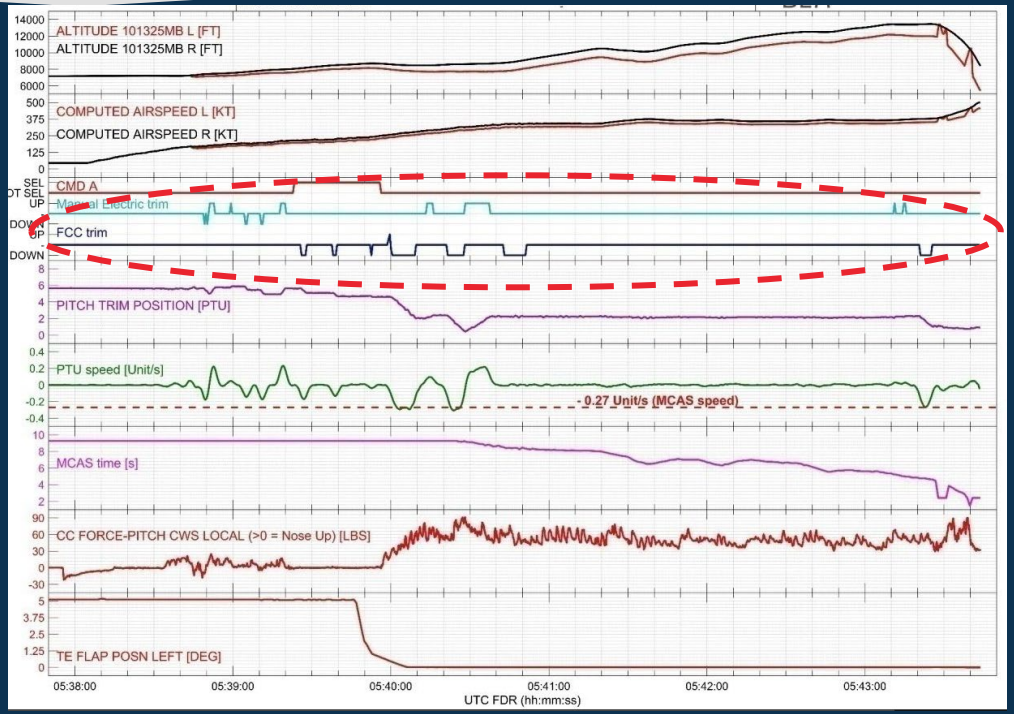

Elevator (Yoke)
Stabiliser – linked to MCAS and flight control system
THE AIR CURRENT

737 Max - MCAS


Stabilizer Trim
Yoke (Elevator)
Stabilizer Trim wheel
Stabilizer Trim cutout

Flight Data Recorders





Lion Air, Indonesia 28 Oct 2018

Ethiopian Airlines, 10 March 2019

737 Max - Summary

- Interface between machinery, technology and the human has gone terribly wrong.
- BBC report May 2019 includes an interview with US pilot Dr Karlene Petitt
  - She fears that as pilots become more reliant on computerised systems, they are losing the skills to fly the planes themselves - and how to respond when things go wrong.

737 – 500, 9 Jan 2021

- Sriwijaya Air flight SJ 182, Boeing 737-500 crashed into the Java Sea 4½ minutes after take-off from Jakarta, Indonesia, leading to 62 fatalities.
- Flight Data Recorder showed an anomaly - gradual reduction in engine thrust from left engine that was under control of the auto-throttle. Right thrust level remained unchanged.
- Disengagement of autopilot at 10,900ft (that would have been compensating for the significant difference in thrust) followed by a sudden roll of the plane to the left to more than 45 degrees of bank before it crashed into the Java sea.
- At least 2 reported problems with the autothrottle prior to this flight.
- More details awaited as the cockpit voice recorder was only just recovered (31/3/21)

Example – Digital Pressure

- 6 months after first installation (1980s):
  - Some high pressure alarms not working despite passing commissioning test
  - Alarm set at full scale (or beyond) – OK with old analogue system
  - Digital system 4-20mA – could not recognise data beyond instrument range (saturation)
  - Simulated signal sent for commissioning and testing (not final element)

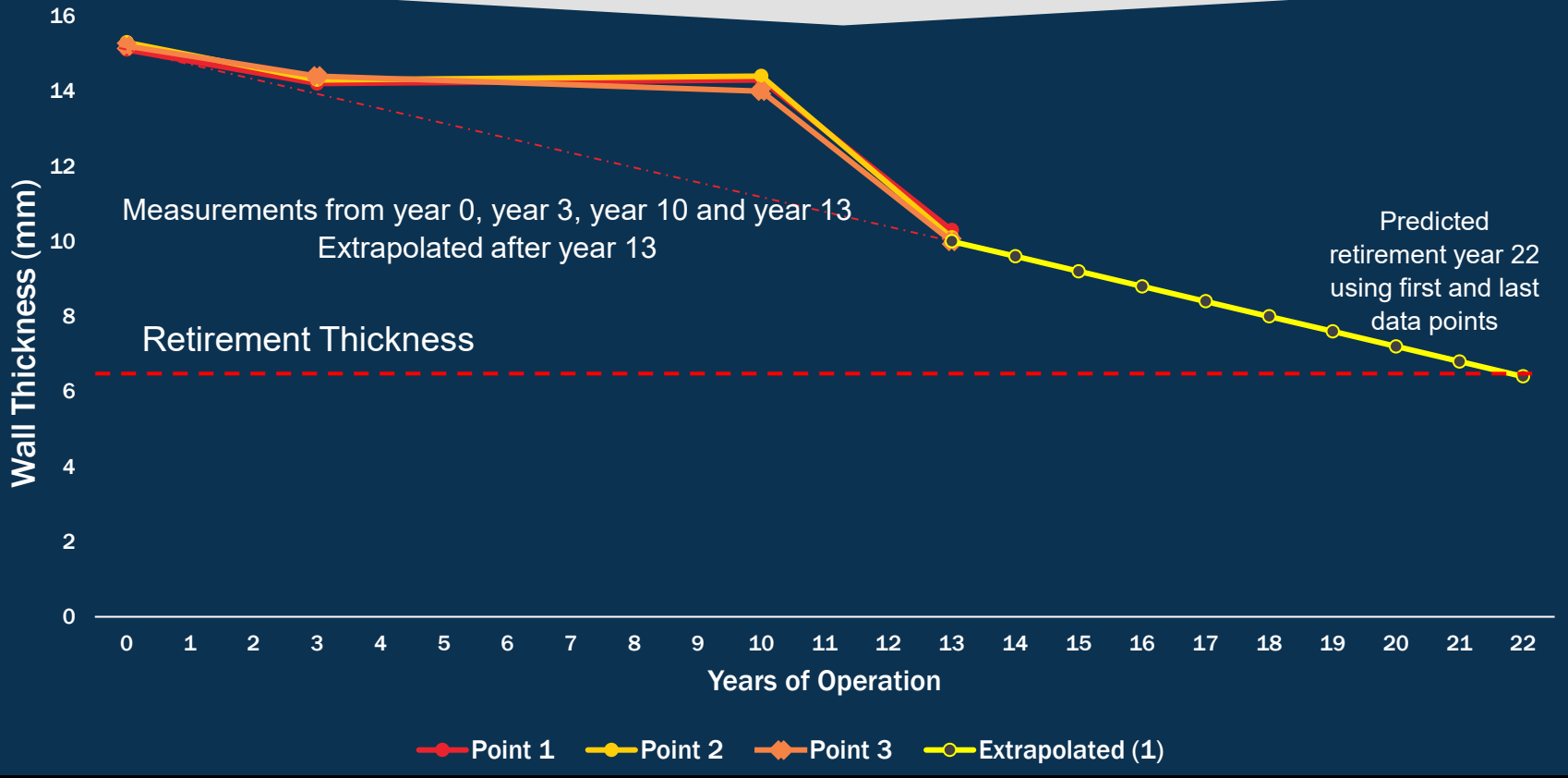
Digital pressure – key issues

- Change of instrument system led to the introduction of a new failure mode that was not realised or understood by the people at the time.
- Key learning point:
  - New technology, especially when associated with safety critical systems, requires a thorough analysis of differences and potential new failure modes.
  - Requires robust MoC system including human factor analysis

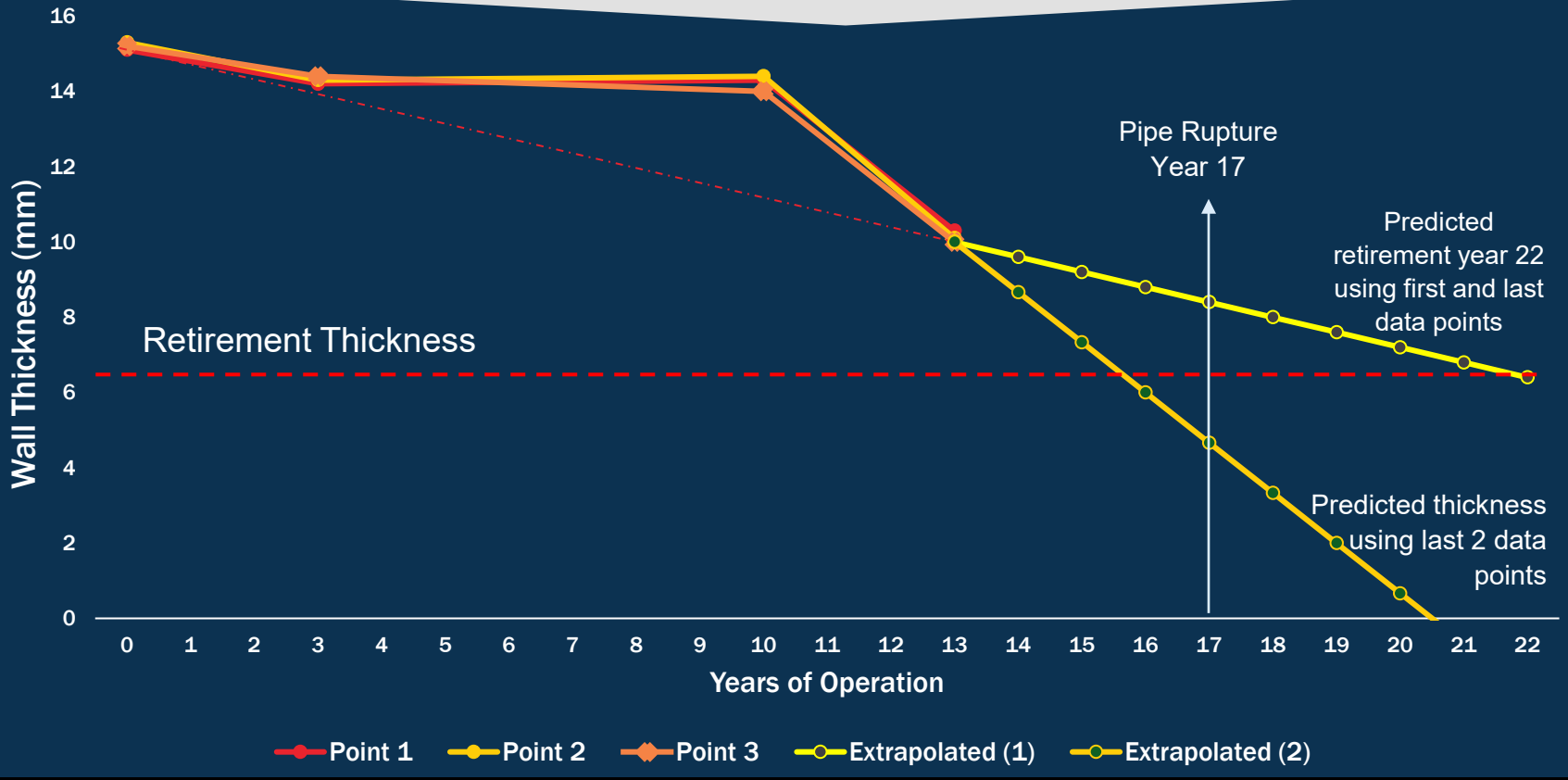
Example – Pipe wall thickness monitoring

- Major Loss of containment and multiple fatalities
- Caused by gradual reduction in pipe wall thickness until pressure could not longer be contained
- Spot measurement/ continuous monitoring at key Thickness Measurement Locations (TMLs) were carried out
- Data used to predict retirement dates using software/ algorithms
- Comprehensive reporting
- 13th year of operation, the thickness checks/ software calculation showed 9 years to go before the retirement thickness reached (total life 22 years)
- Pipe failed after 17 years of service

Example – Pipe wall thickness monitoring



Example – Pipe wall thickness monitoring

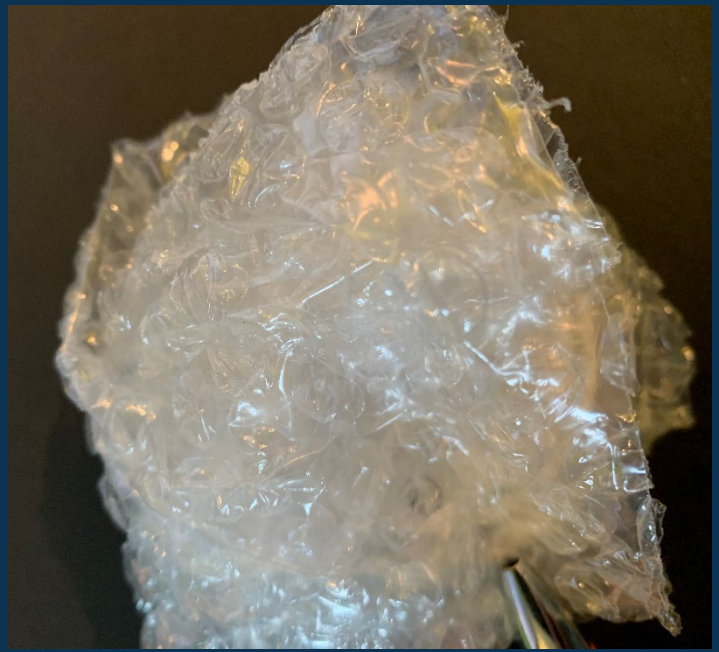


Pipe wall thickness monitoring – key issues

- Maintenance planners not familiar with software
  - Unaware of how columns of data are selected in the program
  - Used to be performed by the engineers (more hands-on)
- Output from the software - tables of data
  - Relied upon for asset replacement decision-making.
  - Lack of plotting of trend data
- Highlights the importance for staff to have a full understanding of new automated systems
  - Since these can also introduce potential new modes of failure.
- Human factors associated with the new system not considered

Bonus Example - The All New DCS

- Introduced in 1970s & 80s
  - Before the concept of alarm management, e.g. IEC 62682
- Easy to add alarms
  - Let's have plenty
- No / limited prioritisation/ hierarchy
- Too many alarms (often not required in certain modes)
- Single level password for override of interlocks
- Alarm siren was silenced



Management of Change and Human Factors associated with New Technologies

New Technology and Management of Change

- Early 1980's – MoC only required if there was a change on the P &ID (!)
- Software changes require MoC
- New technology requires use of robust MoC
  - Replacement in Kind (RIK) not always fully understood - same equipment, different manufacturer, different failure mode?
  - Do we know the failure modes?

New Technology and Human factors

- Are we replacing a human barrier with something more or less reliable?
- What will the human do if/ when the barrier fails to work?
  - Is it understood / too complex?
- Are we transferring a safety critical task to someone else and are there adequate procedures in place to control this
  - E.g. Labelling process equipment using bar codes / NFC
  - End of life prediction via TMLs
- Human Factors in Risk Assessment

Where technological change appears to provide additional safety barriers/ layers of safety, we need to ensure that we are not degrading our existing barriers due to factors associated with human performance.

Testing the Barriers

Testing the Barriers

- Tried & Tested vs new Technology/ Human interface – unknown failure modes
  - Especially where critical safety barriers are involved
- Try out in low risk applications first
  - Consider learning from failure (bottom-up approach) vs perfecting a system design (top down)
  - Black Box Thinking*
- Nuclear site trialling wireless instrumentation?!
  - Tried on non-safety systems first – service accounting etc
  - Identify flaws / reliability/ human factor elements
- Involve operators and maintenance crews in trials
  - Helps identify any human factors that may degrade reliability

* *Syed M., 2016*

Conclusion

- Tempting to rush to adopt new tools and technologies
  - Significant benefits
- Overall analysis required to assess impact on safety critical systems
  - Many of which will involve human factors – people/ equipment / technology
- Use a systems approach for process safety
  - The big picture, looking at whole systems, not just units in isolation
- Make sure the use of modern technology is of benefit and does not have an adverse effect on the overall safety of the system

And Finally

John Aaron, former NASA Apollo flight controller

- Considered responsible for saving Apollo 12 after it was struck by lightning in 1969 at T+36.5 and T+52 seconds
  - "Try SCE to Aux"
- BBC podcast "13 minutes to the Moon", 2019
  - In response to an audience question about the advances in technology in the 50 years since the lunar missions, whether this would make it easier for us to get there next time, or if we now have more hurdles to overcome because we have too much technology in the way?

"Just because you have the technology to make a system complicated, doesn't mean you should."

BAKERRISK®

Identify | Evaluate | Solve

Question Time

www.BakerRisk.com

Copyright BakerRisk. All rights reserved.

Contact Us

Roger Stokes

Regus House, Herons Way
Chester
CH4 9QR

+44 (0) 1244 987801

rstokes@bakerrisk.com

Optional caption, delete if not needed