Human Performance and the Fourth Industrial Revolution

Roger Stokes, Principal Engineer, BakerRisk Europe Limited, Chester

Since the first Industrial Revolution, technology has evolved to provide us with new products and production methods, improved quality, output, efficiency and many other benefits. However, this came at a cost and much has been learnt from incidents where the unexpected or the unforeseen (and perhaps unforeseeable) has happened. The pace of technological change has increased and we are now entering the "Fourth Industrial Revolution." This paper discusses some examples in which introduction of new technology has led to safety issues and incidents, and offers suggestions on what can be done to minimise the risks of technological developments leading to technological disasters.

Introduction

The "Fourth Industrial Revolution," the "Internet of Things," "Digitisation" and "Digitalisation" are upon us, bringing together machines, systems, data, devices and humans that are communicating with each other in ways that are continuously evolving. We live in exciting times and this has the potential to provide huge benefits including increased productivity, efficiency, innovation, safety and ultimately to improve the quality of life for everyone on the planet.

However, in industries where the consequences of failure are severe, this could also introduce unacceptable risks. This is particularly an issue where the potential negative interactions between these new ways of doing things and our existing systems, including human interactions and performance factors, are not fully understood and assessed.

There are many examples where technical progress has led to incidents and much has been learnt to avoid similar failures; however as yet newer technologies come into play, they may introduce new failure modes and types that are difficult to foresee.

This paper is not a guide to these new technologies; more a message to potential users of new technology and tools to adopt a holistic or systems approach that considers the various interactions of humans, machines, and technology. Most Process Safety Management (PSM) systems already include Management of Change (MoC) and this is a good starting point to help ensure that safety, particularly in high hazard industries, is not compromised. Unfortunately, in situations where potential failure modes of systems are not known about or properly understood, there can still be unintended consequences. *You don't know what you don't know (the unknown unknowns).*

This paper includes examples of problems that have been associated with the introduction of new technology and some suggested methods to help prevent similar types of incidents from occurring.

Examples of New Technologies

In process industries, there are many applications where recent technological advances can improve performance, efficiency and safety, including:

- Wearable technology that allows us to continuously monitor what we do, where we are and how healthy we are.
- PPE can include gas detectors and personnel locators that feed data back to the control room and analytics systems.
- Permits to work can be digitised so that everyone has access to them and the system is no longer wholly reliant on a piece of paper in the top pocket of the technician's overalls.
- Locations of maintenance work can be more clearly identified using bar codes/ QR codes and increasingly GPS/ Radio Frequency (RF) devices.
- Process isolations can be made "live" on the DCS so that operators in the control room can see which manual valves are closed.
- Operators and technicians can wear cameras so their supervisor can see what they are doing.
- Checklists for high-risk activities can be completed digitally.
- Digital twins allow operators to be trained on systems that are off-line. Coupled with virtual reality systems, this can lead to faster and more effective training.

Historical Examples of Problems with New Technology

Setting aside examples from the "First" Industrial Revolution, such as boiler explosions, colliery disasters, etc., there are plenty of examples where technical developments have led to unforeseen problems and incidents.

Example 1 – Vehicle Automation

From a personal perspective, I can relate back to my first vehicle. At 17 years old, I became the proud owner of an "H" (1970) registered Austin 1300 GT with a 1275 twin carburettor engine pushing out 56 bhp, as shown in Figure 1. (This one was 7 years old when I bought and it eventually went to the scrapyard).

Figure 1: Austin 1300 GT, circa 1970 (*Car and Classic, 2020*)

The most sophisticated electrical system was the ignition coil and there was a bank of electro-mechanical relays under the bonnet that used to get stuck and needed hitting with a hammer from time to time.

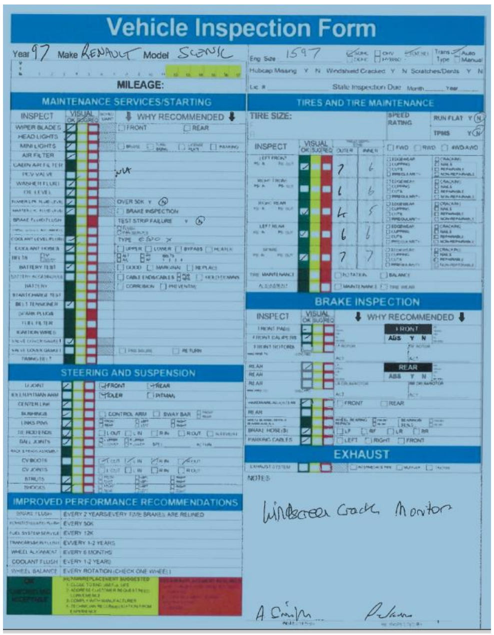
My current vehicle is far more sophisticated and has a feature that automatically turns on the headlights when it gets dark. On the face of it, this is a very helpful device for obvious reasons, but there are two factors that can lead to problems.

a) They also fitted day running LED lights
b) I can turn the headlights off, overriding the "Auto" feature

So, if the lights are turned to the "off" position and it starts to get dark, I can still see alright because the LEDs are on and I forget to turn the headlights on. However, the rear of the vehicle is unlit, an obvious safety issue, which is probably why other drivers keep flashing their lights at me. This is a good example where there is an apparently useful bit of technology, but then you put a human in the way and new, unintended problems occur. A more thorough evaluation of the various interactions of the overall system (including the driver) might have led to simple additional changes, e.g. reset to auto every time you start the ignition.

Example 2 – Checklists

Another example concerns vehicle service checklists. These are given to us as part of the "free" checks that are conducted as part of a service. In the old days, you would receive a slightly oily, handwritten piece of paper that provided some reassurance that the work was actually done (Figure 2). Nowadays, one is more likely to be handed, or emailed, a computer printout (Figure 3). This provides benefits to the garage in terms of more comprehensive, retrievable and auditable records.



Vehicle Inspection Form

Year 97 Make RENAULT Model SCENIC Eng Size 1597

Hubcap Missing Y N Windshield Cracked Y N Scratches/Dents Y N

MILEAGE:

MAINTENANCE SERVICES/STARTING

TIRES AND TIRE MAINTENANCE

TIRE SIZE:

BRAKE INSPECTION

STEERING AND SUSPENSION

EXHAUST

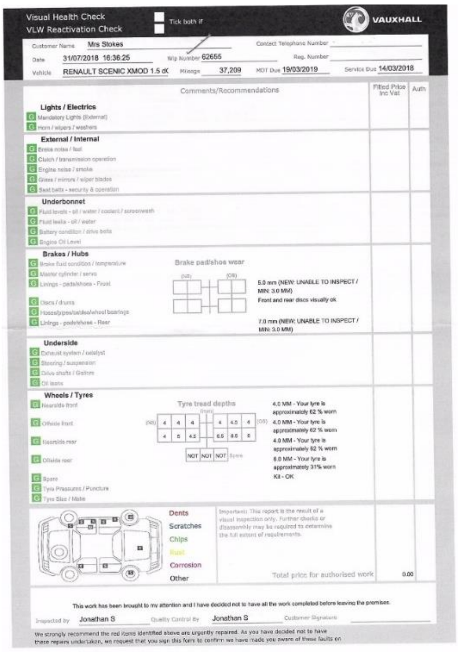
NOTES

Windscreen Crack Monitor

IMPROVED PERFORMANCE RECOMMENDATIONS

BRAKE FLUSH	EVERY 2 YEARS/EVERY TIME BRAKES ARE RELINED
[illegible]	EVERY 50K
FUEL SYSTEM SERVICE	EVERY 12K
[illegible]	EVVERY 1-2 YEARS
WHEEL ALIGNMENT	EVERY 6 MONTHS
COOLANT FLUSH	EVERY 1-2 YEARS
WHEEL BALANCE	EVERY ROTATION (CHECK ONE WHEEL)

Figure 2: Old Service Checklist



Visual Health Check
VLW Reactivation Check
Tick both if

VAUXHALL

Customer Name Mrs Stokes
Date 31/07/2018 16:36:25
Wip Number 62655
Vehicle RENAULT SCENIC XMOD 1.5 dC
Mileage 37,209
MOT Due 19/03/2019
Service Due 14/03/2018

Comments/Recommendations

Lights / Electrics

External / Internal

Underbonnet

Brakes / Hubs

Brake pad/shoe wear

5.0 mm (NEW: UNABLE TO INSPECT / MIN: 3.0 MM)
Front and rear discs visually ok

7.0 mm (NEW: UNABLE TO INSPECT / MIN: 3.0 MM)

Underside

Wheels / Tyres

Tyre tread depths

4.0 MM - Your tyre is approximately 62 % worn
4.0 MM - Your tyre is approximately 62 % worn
4.0 MM - Your tyre is approximately 62 % worn
6.0 MM - Your tyre is approximately 31% worn
Kit - OK

Dents
Scratches
Chips
Rust
Corrosion
Other

Total price for authorised work 0.00

This work has been brought to my attention and I have decided not to have all the work completed before leaving the premises.

Inspected by Jonathan S Quality Control By Jonathan S Customer Signature

We strongly recommend the red items identified above are urgently repaired. As you have decided not to have these repairs undertaken, we request that you sign this form to confirm we have made you aware of these faults on

Figure 3: New Electronic Service Checklist

The green "G" on the electronic checklist means all is well although it does leave one wondering if the service receptionist produced the form using a "tick-all" option. It does not reassure the owner that the work had actually been done. Does the completion of a checklist in electronic format make the system more robust and more likely that it will be properly used?

A paper (*Mosier et al,1992*) involved a trial in the aviation sector on the use of electronic checklists (ECL's) versus manual checklists. Mosier concluded that: *"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. Enough about motor vehicles but more about checklists.

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

Not enough mud was pumped down an underbalanced well whilst drill pipe was removed (a process known as "Tripping"). This led to a blowout and fire that killed five workers. As usual, there were many factors that contributed to this incident. One of them was that there was a new electronic version of a trip sheet, which included a feature that automatically calculated the fluid balance in the well, rather than relying on a manual calculation. Unfortunately, the operator was not trained in the use of the electronic trip sheet and this contributed to the significant gas influx to the well prior to the blowout. The drillers had also turned off the alarm system that was giving excessive nuisance alarms, masking more critical alarms. The CSB report (*CSB, 2019*) states (with sections underlined by the author):

> *"Drillers are trained to monitor whether the well is taking the correct amount of mud while tripping by filling out a "trip sheet," where the calculated volume of the pipe removed is compared to the volume of mud taken by the wellbore. If the actual volume of mud pumped to keep the wellbore full is less than the calculated volume of the pipe being removed, it could be an indication of an influx of formation fluids into the wellbore.*
>
> *Patterson had just started transitioning its drillers to using* ***electronic trip*** *sheets instead of paper trip sheets. The electronic trip sheet had built-in functionalities, including the ability to automatically calculate parameters that the driller would manually calculate using a paper trip sheet. While one driller the CSB spoke with liked the electronic trip sheet because of the ease in populating fields, the driller who worked on the shift before the incident implied that he was not computer savvy and had difficulties with using the electronic trip sheet. The driller had test-used a couple of electronic trip sheets, but this was his second time fully using and relying on the electronic trip sheet during a real tripping operation.*
>
> *The driller told the CSB he had* ***never received formal training on using the electronic trip sheet, instead trying to self-teach himself about it using trial-and-error****. This lack of training, in combination with Patterson not conducting performance assurance to determine if he could use the trip sheet in a practical situation,* ***led to misusing the electronic trip sheet and contributed to the significant gas influx****."*
>
> The result of these errors can be seen in Figure 4.

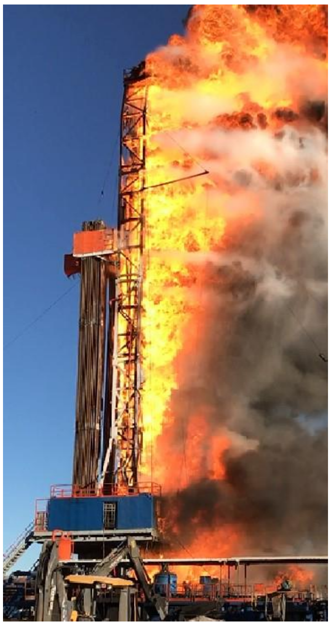


Figure 4: Blowout in Oklahoma

The introduction of a new automated checklist system coupled with apparently inadequate training or understanding of the new system on the part of the operator was a key causal factor with this incident.

A key learning point is that the Management of Change system needs to ensure employees are involved in the details of procedural changes and are properly trained prior to start-up. This is something that one would expect to be checked as part of a Pre-Start-up Safety Review (PSSR).

Example 4 – Boeing 737 Max

The total loss of life from both the Lion Air and Ethiopian Airlines crashes in 2018 and 2019, respectively, was 346 people. This has been widely reported in the media and at the time of writing this paper, the 737 Max aircraft were still grounded following the second crash. There were many causal factors and potential root causes that led to these incidents that will almost certainly be the subject of future case studies.

In brief, the 737 Max was the fourth generation of the 737 that was originally introduced in 1968, before the introduction of sophisticated electronic flight instrumentation systems. The subsequent design iterations included the addition of more sophisticated electronic systems, although the basic flight control systems remained electro-mechanical and hydraulic (rather than full “fly by wire” systems).

Figure 5: Early 737 200 model *(Airways Magazine, 2020)*

Figure 6: 2018/2019 Model 737 MAX *(MRO-Network.com, 2020)*

A key factor that was common to both disasters was a new automated system, MCAS (Manoeuvring Characteristics Augmentation System) that was installed to counter, automatically, a nose-up tendency that arose due to the requirement to mount the more efficient (and larger diameter) CFM engines slightly further forward and higher up under the wing (Figures 5 and 6). The MCAS system activates if a single angle-of-attack sensor (Figure 7), which operates on the same principle as a weathervane, goes beyond a pre-set limit, depending on airspeed, altitude and flaps settings. The provision of this system was advantageous to Boeing and the airlines/pilots since it prevented the Max from having different handling characteristics to that of its predecessors.

Figure 7: Typical angle-of-attack sensor

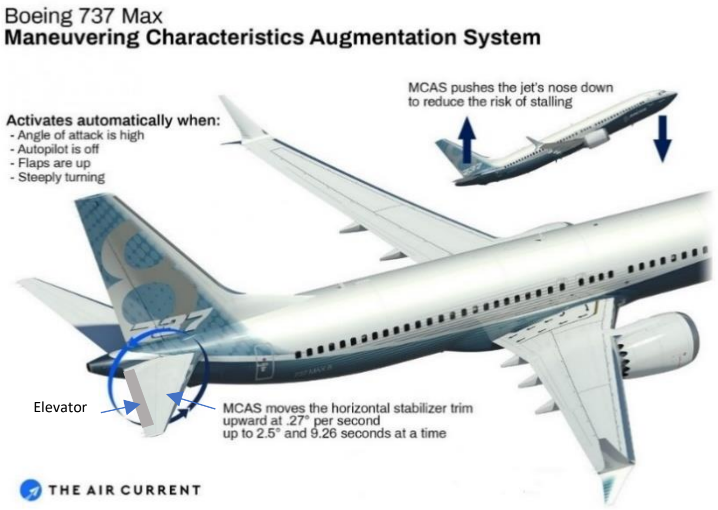


Figure 8: MCAS explained *(The Air Current, 2019)*

In both cases, the MCAS system (Figure 8) activated erroneously, due to a fault with the single angle-of-attack sensor. In the case of the Lion Air incident, it could have involved a mis-calibration following a repair and with the Ethiopian incident, it might have been a bird-strike. With the stabilizer trim bar tilting the nose down, in both cases the pilots fought to maintain level trim by pulling on the control column, which lifts the elevator, located behind the trimmable stabilizer. They also countered the automatic movement of the stabiliser trim by using an electric trim switch on the control column to drive the trim in the nose-up direction. However, unless the MCAS system is then switched off, it repeats the nose-down movement.

Figures 9 and 10 contain flight data recorder (FDR) information for the two 737 Max crashes.

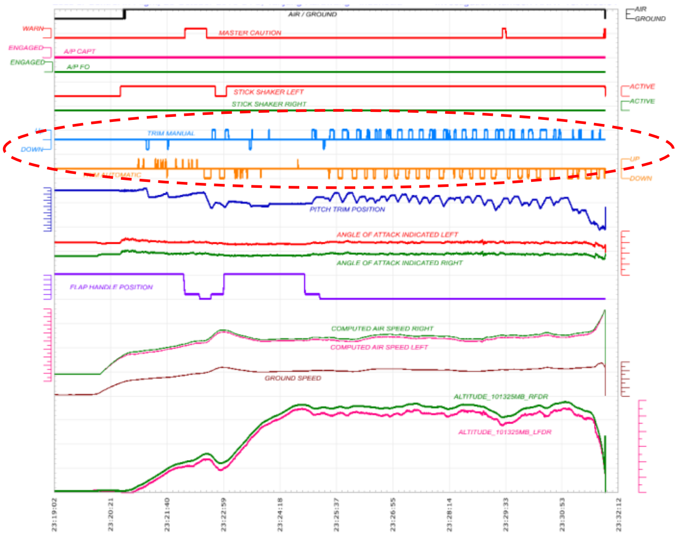


Figure 9: Lion Air FDR, Indonesia 28 October 2018 *(Figure illustrating FDR data, Tjahjono, S. et al, 2018: p.14)*

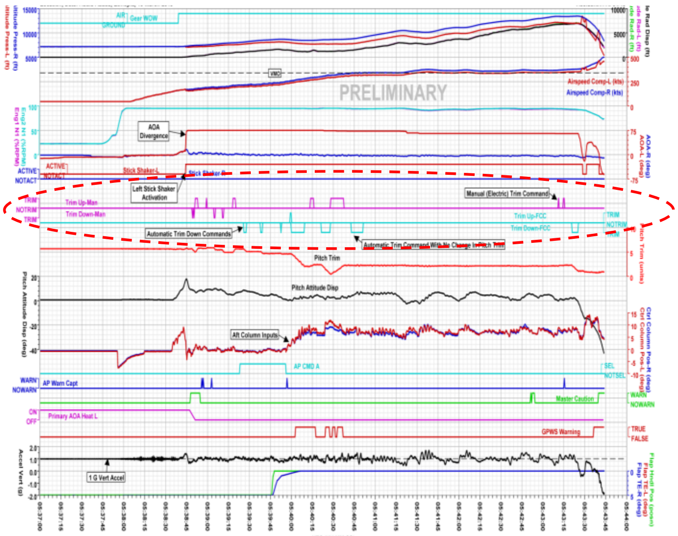


Figure 10: Ethiopian Airlines FDR 10 March 2019 *(Figure illustrating FDR data, Ethiopian Ministry of Transport Aircraft Accident Investigation Bureau, 2019, p. 26)*

In the case of Lion Air, the flight crew countered the MCAS activation using electric trim over 30 times before the crash (Circled in Figure 9). The Ethiopian flight crew countered it twice (Circled in Figure 10) before following a “runaway trim” procedure and isolating the automatic system. This procedure was emphasised by Boeing who issued an Operations Manual Bulletin dated November 6, 2018, after the Lion Air crash *(Section 5.11, Tjahjono, S. et al, 2018, pp 51-52)*. However, in the case of the Ethiopian flight, after isolating the electrical trim system, the control surfaces were out of trim (“mistrim”), and the crew had to counter the forces on the horizontal stabilizer trim by pulling back on the control column. It appears that they tried using manual trim wheels to trim back the horizontal stabilizer, but it has been suggested *(Gates D., Seattle Times, 3 April 2019)* that the forces on the control surfaces were too great for them to achieve this. Eventually they de-isolated the automatic trim system and applied some electric trim. However, this allowed the MCAS system to cut in again and automatic nose down was applied leading to a steep dive (with negative g-forces) some 20 seconds before the crash.

Key fundamental issues were *(Travis G., 18 April 2019)*:

- The 737 Max design, that led to the tendency to pitch up
- The installation of an automated system intended to alleviate that tendency
- Its reliance on a single sensor that did not cross-check with another sensor

There were many other direct and indirect causes of these two incidents, including pilot training and there are suggestions that root causes lie deep in leadership and cultural issues within the industry; matters that go way beyond the scope of this example.

This is a tragic case where the interface between machinery, technology and the human has gone terribly wrong. A BBC report in May 2019 includes an interview with US pilot Dr Karlene Petitt *(Leggett, T. (BBC), 17 May 2019)*. 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.

Learning points are still being evaluated at the time this paper was written, although they are likely to involve most of the elements of a typical PSM system. (*CCPS, 2007; Energy Institute, 2010*).

Example 5: Digital Pressure

Referring back to the process industries, during the 1980’s, one chemical manufacturing site started to introduce digital pressure gauges (Figure 12) to replace the analogue ones (Figure 11).

Figure 11: Analogue pressure gauge and alarm

Figure 12: Digital pressure gauge and alarm

About six months after several of these were installed, the site issued a safety bulletin about the high pressure alarm settings. On the old analogue instruments, it was not an issue if the alarm was set at full scale (or even slightly beyond) but with the digital systems operating at 4-20mA, there were cases where it would allow the high alarm to be set just out of range (saturation), which negated its function. However, it passed a commissioning test that involved the use of a simulated signal sent to the alarm. The problem was only discovered when a final element test was conducted after the system had been in operation for some time, clearly without a functioning high pressure alarm/trip.

The change of the instrument system effectively led to the introduction of a new failure mode that was not realised or understood by the people at the time. A key learning point is that the new technology, especially when associated with safety critical systems, requires a thorough analysis of differences and potential new failure modes. Again, these factors would be properly considered via a robust MoC system.

Example 6 – Furnace Explosion

Another example in the process industry associated with introduction of new instrumentation systems involves a large gas-fired furnace. The instruments and controls were gradually upgraded over a period of time and eventually, during a turnaround, the control panels were updated. The project was behind schedule and there had not been an opportunity to train everyone on all of the features of the new panel. Shortly after start-up, there was a power dip and the furnace tripped out.

The start-up procedures called for the furnace to be air-purged to remove any flammable gases and for a supervisor to carry out a physical check of the valve position of each of the 12 or so gas valves to ensure they were all in the closed position. However, for the first time in the history of the plant, the system was able to show the position of each of the gas valves from the control room. The supervisor considered that it would be reasonable to check the control panel rather than conduct a physical inspection of the valve positions on the site. Unfortunately, one of them was not fully closed and although the panel showed that this was the case, the supervisor misread the panel and thought they were all closed. When the furnace was ignited, there was a major explosion that destroyed the furnace and the tubing inside.

It was never the intention that the new control system precluded the requirement to physically check the gas valve positions and the indication on the panel was not particularly clear. In this case, the human factor element is key, particularly without the training or the opportunity for the supervisor to discuss the operation with the new technology. A root cause analysis would not attribute the cause of the incident to the supervisor, but rather to the management system. A good PSM system would include a requirement for a Pre-Start-Up Safety Review (PSSR) as part of the new systems, including confirmation of the provision of necessary employee training.

Example 7 – Condition Monitoring - Pipe/ Vessel Wall Thickness

Measurement of piping and vessel wall thickness in order to estimate end of life is a key barrier in preventing loss of containment (LOC) events. There are several new products available to carry out continuous measurement at key thickness measurement locations (TMLs). Software can be used to calculate rates of thickness loss, both on a short-term and long-term basis and to provide alarms if there are sudden changes. Comprehensive reporting can be automated, inspection intervals can be set and retirement dates estimated. The advantages of these tools and techniques are clear but this example demonstrates how such a system could introduce a new potential weakness in the asset integrity system.

The user of the software was able to select the data points to calculate the estimated retirement date of the asset. In the 13th year of operation of the pipeline, the thickness checks and the software calculation showed that there was another 9 years to go before the retirement thickness was reached. Trend data was not plotted.

The pipe ruptured in the 17th year of service resulting in an LOC, major vapour cloud explosion and multiple fatalities. The investigation found that a causal factor involved the way the data was selected via the software for calculating the retirement date.

The very first and the most recent data sets had been selected, which gave an estimated retirement date in year 22. However, the corrosion rate had increased in recent years, and had the last two data points been used, the retirement date would have been given as year 16 and various warning flags would have been raised before the failure occurred. This is demonstrated by the graph in Figure 13, where the blue line (Extrapolated 2) shows a much higher rate of metal loss than the yellow line (Extrapolated 1).

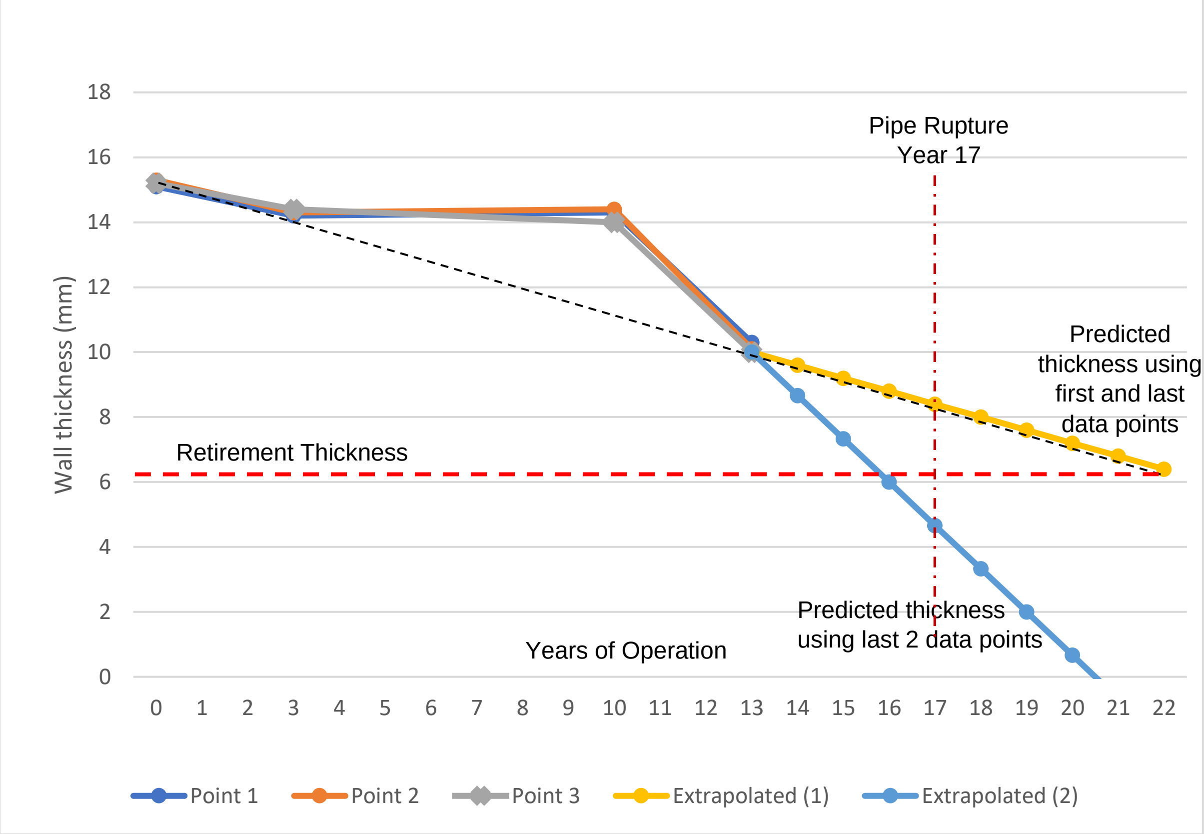


Figure 13 – Trend data for metal wall thickness measurements

The engineers were apparently unaware of the way the columns of data had been selected in the program (possibly by a supervisor who was not fully aware of the criticality of the data selected) and the output from the software, in the form of tables of data, was relied upon for asset replacement decision-making. Human factors associated with the selection of applicable data for trend plotting resulted in the failure to accurately predict end of life. The lack of plotting of trend data was also factor in the issue being hidden from the engineers.

This example shows how important it is for staff to have a full understanding of new automated systems since these can also introduce potential new modes of failure. This may include initial and periodic manual validation on safety critical systems.

Management of Change and Human Factors associated with New Technologies

The process industry has developed and evolved the MoC definitions and requirements over many years to consider issues that have arisen and through learning from incidents where poor change management was a causal factor.

Before the 1980s, some companies considered that MoC was only required if there was a change to a Piping and Instrument Drawing (P&ID). Then computer control software arrived and it was clear that changes to software needed to be included. Companies refer to Like-for-like or Replacement in Kind (RIK); terms that are used but not always clearly defined or understood by the key people involved.

A good MoC procedure should ensure that anything more that an “identical” change requires a formal safety review. There should even be a review of an “identical” change, to confirm that there are indeed no changes. Replacement of an instrument with an apparently identical one supplied by another manufacturer may present different failure modes from the original and these also need to be evaluated.

Minor changes or an apparent enhancement to equipment, procedures or organisations all require a level of structured risk assessment. The principle of inherently safer design and “*the avoidance of hazards rather than their control by added protective equipment”* (*Kletz, 1998*) should always be considered when making changes to systems. The structure and operation of a good

MoC procedure is beyond the scope of this paper. Details are provided by the Health and Safety Executive (*HSE, 2020*) and it is a key element of process safety management systems as provided by the Center for Chemical Process Safety (*CCPS, 2008; 2020*) and the Energy Institute (*Energy Institute, 2015*).

Installation of new technologies that are designed to add to the layers of protection may, under certain circumstances, have the opposite effect. Whilst on the surface the potential for improvements in safety may be clearly visible, it is extremely important to recognise that human performance may alter when using this technology. For example:

- Does a digital checklist, where boxes are clicked via a smartphone (and there may be a "tick-all" option) make it more or less likely that the user will indeed carry out all the checks than the old pen and paper system?
- If a manual process isolation is shown "live" on a display in the control room, will this make it less likely that an actual physical check is carried out on the plant?
- If the operator has a wearable camera that streams back to the control room, does this satisfy the "four-eyes" principle that many companies use for high-risk operations?
- Will the operator know what to do if/when the digital system fails?
- Would such improvements be recognised as changes and receive an appropriate level of scrutiny via a management of change process that includes their impact on human performance?

It could be considered that *the more help you give people, the more they don't do for themselves.*

Management of Change procedures should also include consideration of Human Factors associated with the change. Some further examples follow:

- The installation of a high level trip on a storage tank would appear to be a sensible precaution to prevent overfill. It would seemingly provide an additional layer of protection to the existing one that was based on operators being extremely vigilant; including calculation of fill times and when inlet valves need to be closed. Without additional measures, the operators may decide to abandon their previous methodology (that had been extremely reliable over the years) and wait for the high level trip to operate. The reliability of the instrument may be high, but is it as reliable as the operators used to be? In this example, sensible additional measures could include collection and review of data on high level trip activations.
- If we are now using video monitoring to ensure the fitter has gone to the right pump, can we now stop sending the operator out to the plant to verify the location? Which system is more reliable and what are the possible failure opportunities for the video system (e.g. inability to see pump number; identical pumps in different locations, etc.)? These issues would need to be evaluated as part of the change procedure.
- If we start to use digital labelling (bar-code/ NFC) for tradesmen to correctly identify equipment location, how do we eliminate the possibility of the person who labels the equipment fitting it in the wrong place? What happens when the label falls off or is painted over? A robust procedure is required for reliable management of the labelling systems.

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

High hazard process industries are traditionally very conservative in adopting new techniques and technologies. This is for good reason as we do not want to replace tried and tested systems with ones where the integrity/ reliability, including the effect of human performance on these new systems, is not fully understood. This is even more important where critical safety barriers are involved, including control/shutdown systems or working practices, such as isolation for maintenance.

It was therefore surprising to hear that in 2016, a nuclear site was trying out wireless instrumentation. Concerns were reduced significantly once it became apparent that they were trialling the devices on non-safety related systems such as services accounting flowmeters (steam/ water etc.) Their plan was to monitor the performance and accuracy of these systems for a number of years, to identify any flaws and reliability issues that they exhibited.

Perhaps this approach is a sensible way forward when considering the adoption of new technology in more safety-critical systems. Whilst a complex analytical approach could be used to evaluate reliability of individual items of equipment, it may not necessarily pick up all of the human factors or other elements of the overall systems that are associated with the change. An alternative method would be to test the equipment in a low risk application (and with the ability to turn it off!), investigate and correct failures and establish reliability of the overall system, including the associated human factors that may degrade the reliability of the equipment. Such an approach is discussed in the text *"*Black Box Thinking*" (Syed M., 2016)* that emphasises the benefits of learning from failure (a bottom-up approach) rather than trying to perfect the design of the system using a top-down methodology. He cites Dyson's 5,127 "failures" in cyclone vacuum cleaner prototypes before the final design was adopted.

Conclusion

Whilst some companies will rush to adopt the new tools and technologies, it is suggested that a more detailed analysis of the overall systems be conducted before implementation on safety-critical systems and procedures/ work practices.

Our new IChemE President, Stephen Richardson, gave an inaugural address entitled: *Process safety: the big picture and the systems approach,* which focussed on the need to look at whole systems, instead of units in isolation, to ensure that plants, programmes and processes are working efficiently and safely *(IChemE, 13 Nov 2019)*. This approach is key to ensure that use of modern technology is of benefit and does not have an adverse effect on the overall safety of the system.

The law firm Kennedys wrote an article on this topic:

> *As technology continues to develop, there will no doubt be considerations for the regulatory authorities including the HSE as to their approach in their investigation and relevant parties to pursue following an incident. In the meantime, businesses may wish to proceed with caution with a view to avoiding any over-reliance on new technological devices and innovations now at our disposal. Technology should be regarded as a useful additional aid to oversee health and safety within the work place, rather than a replacement for a trained, competent workforce with suitable and sufficiently documented systems of work. (Holbrook, J., 13 Dec 2018)*

Inherently safer design principles should be considered before changes are made to software or other controls.

The twelfth episode of the 2019 BBC podcast "13 minutes to the Moon" *(BBC Podcast, 2019)* was recorded at Rice University Football stadium in Houston and includes an interview with John Aaron, who was an Apollo flight controller at NASA in Houston with responsibility for electrical, electronic and life support systems of the command module for the lunar landing. He was considered responsible for saving Apollo 12 after it was struck by lightning and later in his career worked on the space station project. In response to a question from the audience 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, Aaron responded:

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

This paper is intended to provide some guidance on safety issues related to the introduction of new technologies in the process industry. Whilst it does not provide answers to specific problems, hopefully it gives some useful information and advice on how to manage and implement these changes by considering the system as a whole. The way humans react and behave alongside technological developments must be considered a key part of the Management of Change process.

References:

Airways Magazine, 2020, *Flashback: When Southwest Retired The Boeing 737-200,* photo, 737-200, Available from: https://airwaysmag.com/airlines/flashback-when-southwest-retired-the-boeing-737-200, [Accessed 2 January 2020]

BBC Podcast, 2019, *13 minutes to the Moon*, Available from: https://www.bbc.co.uk/programmes/w13xttx2/episodes/downloads, [Accessed 2 January 2020]

Car and Classic, 2020, *Austin 1300 GT – Fully Restored Example SOLD,* Available from: https://www.carandclassic.co.uk/car/C908726, [Accessed 2 January 2020]

CCPS, 2007 *Guidelines for Risk Based Process Safety*

CCPS, 2008, *Guidelines for Management of Change for Process Safety*

CCPS, 2020, *Introduction to Management of Change,* Available from: https://www.aiche.org/ccps/topics/elements-process-safety/manage-risks/management-change/introduction, [Accessed 2 January 2020]

CSB, 2019, *Gas Well Blowout and Fire at Pryor Trust Well 1H-9,* Available from: https://www.csb.gov/pryor-trust-fatal-gas-well-blowout-and-fire, [Accessed 2 January 2020]

Energy Institute, 2010, *High level framework for process safety management*

Energy Institute, 2015, *Guidance on meeting expectations of EI Process safety management framework Element 12: Management of change and project management*

Ethiopian Ministry of Transport Aircraft Accident Investigation Bureau, 2019, Federal Democratic Republic of Ethiopia, *Aircraft Accident Investigation Preliminary Report Ethiopian Airlines Group B737-8 (MAX) Registered ET-AVJ,* Available from: https://reports.aviation-safety.net/2019/20190310-0_B38M_ET-AVJ_PRELIM.pdf, [Accessed 2 January 2020]

Gates D., Seattle Times, 3 April 2019, *Why Boeing's emergency directions may have failed to save 737 MAX*, Available from: https://www.seattletimes.com/business/boeing-aerospace/boeings-emergency-procedure-for-737-max-may-have-failed-on-ethiopian-flight, [Accessed 2 January 2020]

Holbrook, J., 13 Dec 2018, *Technology and health and safety in the workplace: an aid not a replacement,* Available from: https://www.kennedyslaw.com/thought-leadership/article/technology-and-health-and-safety-in-the-workplace-an-aid-not-a-replacement, [Accessed 2 January 2020]

HSE, 2020, *Plant modification / Change procedures*, Available from: https://www.hse.gov.uk/comah/sragtech/techmeasplantmod.htm, [Accessed 2 January 2020]

IChemE, 13 Nov 2019, *New IChemE President focusses on systems thinking and the big picture for process safety*, Available from: https://www.icheme.org/about-us/press-releases/new-icheme-president-focusses-on-systems-thinking-and-the-big-picture-for-process-safety, [Accessed 2 January 2020]

Kletz T.A, 1998, *Process Plants: A Handbook for Inherently Safer Design*

Leggett, T. (BBC), 17 May 2019, *What went wrong inside Boeing's cockpit?,* Available from: https://www.bbc.co.uk/news/resources/idt-sh/boeing_two_deadly_crashes, [Accessed 2 January 2020]

Mosier, K.L. et al., 2016, Electronic Checklists: Implications for Decision Making, *Proceedings of the Human Factors Society 36th Annual Meeting, Atlanta, Georgia, 12th-16th October 1992.*

MRO-Network.com, 2020 *Boeing Defends 737 MAX Information Handling,* photo, 737 Max, Available from: https://www.mro-network.com/manufacturing-distribution/boeing-defends-737-max-information-handling, [Accessed 2 January 2020]

Syed M., 2016, *Black Box Thinking: Marginal Gains and the Secrets of High Performance: The Surprising Truth About Success*

The Air Current, updated 17 November 2019*, What is the Boeing 737 Max Manoeuvring Characteristics Augmentation System?,* Available from: https://theaircurrent.com/aviation-safety/what-is-the-boeing-737-max-maneuvering-characteristics-augmentation-system-mcas-jt610, [Accessed 2 January 2020]

Tjahjono, S. et al, 2018, *Preliminary KNKT.18.10.35.04 Aircraft Accident Investigation Report, PT. Lion Mentari Airlines, KNKT Indonesia,* Available from: https://reports.aviation-safety.net/2018/20181029-0_B38M_PK-LQP_PRELIMINARY.pdf, [Accessed 2 January 2020]

Travis G., 18 April 2019, *How the Boeing 737 Max Disaster Looks to a Software Developer*, Available from: https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer, [Accessed 2 January 2020]