By Roger Ford – Modern Railways, January 2021 - In Rudyard Kipling's poem 'M'Andrews hymn', an old Scots ship's Chief Fleet Engineer approaching retirement looks back on a long career. His reveries include the developments in propulsion machinery – Kipling knew his engineering – and concludes:

'What I ha' seen since ocean steam began Leaves me na doot for the machine: but what about the man?'

In the 21st century, the same question can be asked about digital control systems and automation. Consider, for example, civil aviation.

Skills

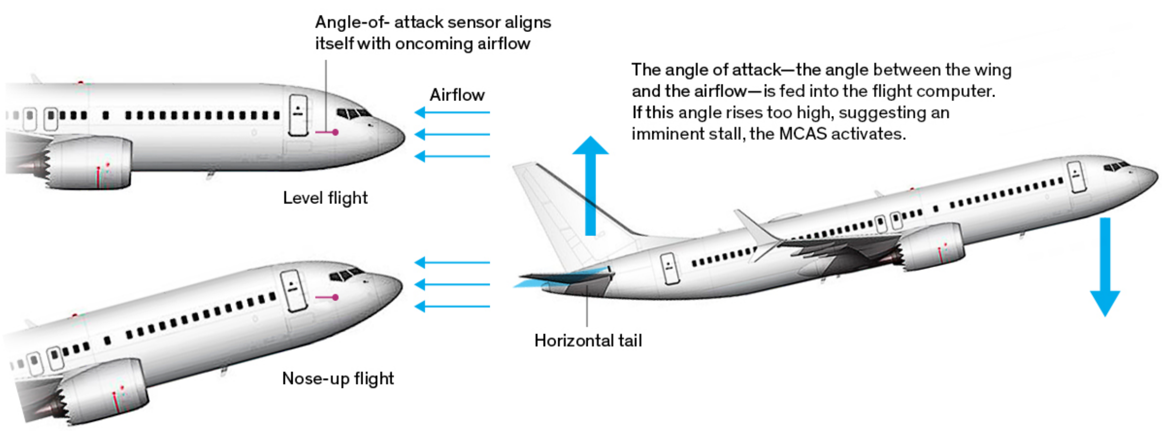
Where once the auto-pilot, originally known as George, maintained straight and level flight on a constant course and at constant altitude, modern Flight Control Computers (FCC) can fly an Airbus or a Boeing more accurately and efficiently than a human pilot. Indeed, for the sake of minimising fuel consumption, captains are instructed to switch on 'the magic' immediately after take-off.

These fly-by-wire flight control systems keep the aircraft within safety envelopes and can override inappropriate control inputs. They are several times safer than analogue flight. But the corollary, the subject of much concern, has been a loss of old-fashioned hand flying skills.

A classic example was Air France Flight 407 (AF407). At 35,000 fleet the autopilot disengaged, assumed to be due to the pitot tubes, which supply air speed indication, icing up. The pilot in control began flying manually and instead of maintaining straight and level initiated a steep climb which turned into a stall. An airliner, with six miles of sky below it in which to recover, crashed into the sea, still in a stall.

More recently, there were the two Boeing 737MAX accidents, where the magic included a facility which Boeing thought the pilots didn't need to know about. To overcome different aerodynamic characteristics resulting from the bigger engines fitted to the MAX iteration of the 737, the flight control software included a programme which trimmed the aircraft nose down if the angle of attack, the degree of nose-up attitude in a climb, exceeded a pre-set amount. This was the Manoeuvring Characteristics Augmentation System, or MCAS. A faulty Angle of Attack (AoA) indicator exaggerated the climb angle and the MCAS responded by pushing down the nose. The pilots manually pulled the nose up, only for MCAS to push it down again.

How the new Max flight-control system (MCAS) operates to prevent a stall



©2020 EngPro Solutions Ltd.

How had this got round the regulators? Well, they were persuaded that pilots would recognise the repeated nose down inputs as a runaway elevator trim motor. The official reaction was to switch off the electric trim and then wind off the nose-down trim manually, using a hand wheel between the pilots' seats. On the previous flight of one of the aircraft which crashed, it had taken the crew over three minutes to work out what was happening and take corrective action. That flight landed safely.

Off the rails: Azuma No 800109 outside Neville Hill on 14 November 2019, the day after the accident. Ian Lyall

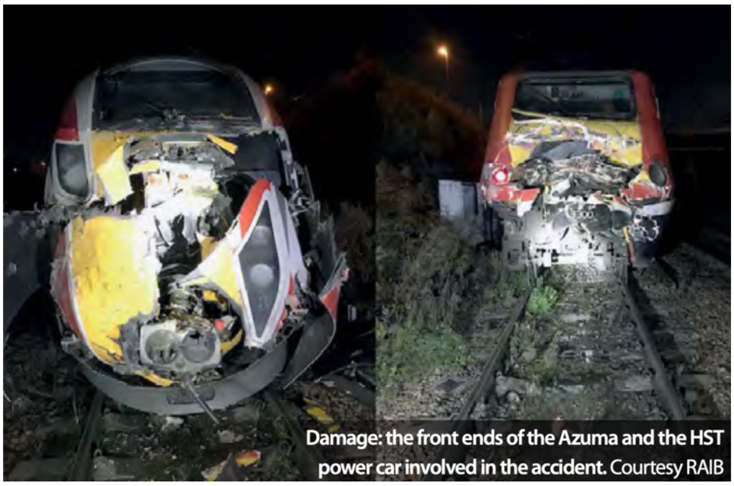
As an aside, for those of us in the technically 'backwards' railway industry, used to the triple redundancy of Solid State Interlockings, for example, the fact the MCAS depended on the input from a single AoA device is hard to understand.

Magic trains

Today's trains are similarly full of 'magic'. And the magic interfaces with the human Mk 1 wetware through the Driver Machine Interface (DMI) – better known as the Train Management System (TMS) touchscreen.

Of course, the magic is not so clever, or potentially as dangerous, as the MCAS in the 737MAX. But it is still pretty bright. For example, take the Class 800 bi-mode, where you need to make sure the pantograph is down when the diesel engines are running and only raised when there is a contact wire above.

Even well-trained professional drivers can make mistakes. And to avoid pantographs waving in the breeze and whacking bridges in non-electrified sections we have the APCO – or Automatic Power Change Over facility – in the TMS. Automatic changeover is triggered by track-mounted beacons, or balises.



Damage: the front ends of the Azuma and the HST power car involved in the accident. Courtesy RAIB

©2020 EngPro Solutions Ltd.

APCO

Sensibly, the default setting for the APCO is 'on'. But it can be switched on and off using the TMS touchscreen. Now for a little bit of train magic. APCO control of the pantograph and engines is determined by the train's four-digit alphanumeric reporting code. The TMS uses this headcode to determine the starting location, destination and the route in between, including scheduled stops.

Where the magic happens: Azuma cab. This is one of LNER's electric versions, No 801108, rather than the bi-mode involved in the Neville Hill incident. Philip Sherratt

When it reads an APCO balise, the TMS uses the route information in its database, which includes the location of electrified sections of line, to determine whether to initiate an APCO intervention; either shut down the diesel engines and raise the pantograph or vice versa. But if the TMS doesn't have a valid headcode, and is running under electric traction, when the train passes a balise the APCO lowers the pan and fires up the MTU power packs, just to be on the safe side.

APCO Trap

Leaving Leeds station to enter Neville Hill depot there is an APCO balise protecting the end of electrification on the main line. However, the wires continue into the depot. On 11 November 2019, a driver, who had just returned to the footplate after a spell off work and was working a Class 800 unaccompanied for the second time, kept the headcode (1D29) of his incoming London to Leeds service for the short run into Neville Hill. What he should have done was insert the headcode (5D29) for the Empty Coaching Stock (ECS) move between station and depot.

As his train passed over the balise, APCO noted the invalid headcode and initiated a power changeover, starting up the diesel power packs. The first the driver knew of it was when the electric power supply indicator on his desk went out and the TMS screen told him the power changeover was completed. This was worrying, because power unit supplier and maintainer MTU doesn't like its engines starting without the oil and coolant being preheated. The driver was concerned his error might be flagged up to Hitachi. A subsequent discussion with his driver manager confirmed entering the ECS headcode for the depot run was required to prevent a recurrence of the APCO annoying the engines.

Headcode insertion

Next day, the driver was back on magic-free IC125 driving duties, but on 13 November he once again brought 1D29 back to Leeds. As before, the final duty was an ECS working as 5D29.However, when the driver tried to enter the ECS headcode he was unsuccessful. Instead, he isolated the APCO and passed over the balise uneventfully.

He was following an IC125 into the depot and stopped for just over a second before the train in front was on the move again. Keen to reinstate the APCO, the driver started to use the TMS. At the same time, he saw the IC125 moving and selected a low level of tractive effort, intending to crawl along behind it while continuing to use the TMS. Having reinstated APCO, which took about 20 seconds, the driver looked up and realised he was going much faster than expected and ran into the rear of the IC125 at 15mph.

©2020 EngPro Solutions Ltd.

Concern

Why was the driver using the TMS? Although he could not explain the decision, the Rail Accident Investigation Branch report into the incident posits that he might have been concerned about forgetting that he had isolated APCO, and that this might not be obvious to the next driver taking over the train.

FIGURE 3: TMS HEADCODE SCREEN

LNER drivers had been taught that 'it is imperative that APCO is reinstated once well clear of the affected area, otherwise it will remain inconspicuously isolated (even after the DDS (Driver Display System) and master switch is turned to OFF)'. RAIB explains LNER had been concerned that a dormant isolation would lead to the next driver having an incident. An APCO isolation would not be immediately obvious on the TMS screen and a driver would need to work down through several sub-menu levels before being able to establish whether APCO was isolated.

However, that possibility had been corrected with a software update a few days earlier. This added a prominent indication 'APCO isolated' to the TMS home screen. A driver also received a warning that APCO was isolated when starting a train using the master switch.

Shades of MCAS

But, as RAIB explains, the driver was unaware of this new feature because he had not been briefed by LNER on the introduction of the software update. This was despite LNER and Hitachi having an engineering change management process for such updates, which would normally have seen drivers receive a briefing on the changes.

RAIB notes that 'in this instance, it appears that the importance of this information was lost in the vast array of changes introduced in this particular software update. It is possible that, if a more thorough description of the change had been included in Hitachi's engineering change pack, its relevance would have been more easily identified'.

Lack of information on this vital change explains the driver's concern with reinstating the APCO. But why did he have to isolate the APCO in the first case? And now we come to the critical interface where the machine betrayed the man.

Having entered the new head code on the TMS screen (Figure 3), the driver appears to have a choice. Either use the 'CHECK STOPS' button, to see the stopping pattern associated with the service he has just inserted, or use the 'HOME' button to complete the change and return to the home screen Since this was an ECS working into the depot, there was no need to check stops and the driver pressed the 'HOME' button. Only to find that the original headcode was still displayed.

©2020 EngPro Solutions Ltd.

Ambiguous

LNER had trained its drivers that pressing CHECK STOPS would allow a driver to check the station stops for the journey ahead. The driver operating instructions identified this as a step in the cab setup process. But drivers were also told that pressing HOME on the headcode screen would take the TMS to the home screen with the headcode having been accepted. However, reveals RAIB, LNER did not understand that CHECK STOPS had to be pressed first for the headcode to be accepted.

This fundamental misunderstanding is attributed 'principally' to the train operation manual supplied by Hitachi, plus a tablet app replicating the behaviour of a Class 800 TMS. LNER based the training courses for its drivers on the operation manual plus another document, the 'TMS screen specification for train crew'. This describes each TMS screen individually and explains the effects of pressing each button on each screen.

RAIB reviewed both documents and concluded that neither 'clearly conveys the message that CHECK STOPS has to be pressed on the headcode screen for the TMS to accept the headcode'. It adds that the Hitachi documentation 'was ambiguous in this regard'.

Been there?

I'm sure that readers will have grappled with ambiguous procedures, buttons and sequences when setting up computers and smartphones. But this was a real lulu. As you can see from Figure 3, CHECK STOPS looks like an option. But if it was an essential action when resetting the headcode, there should have been a NEXT button which would take you to the CHECK STOPS screen, which would have a DONE or FINISHED button.

It is an ergonomic mess, compounding the misunderstanding of the correct sequence in the documentation. How could this have happened? A good question. The same documents used by LNER to develop its training course and its driver operating instructions were also used both by the company developing the Class 800 full-cab driving simulator for LNER and the company commissioned by Hitachi to develop the app replicating the behaviour of the TMS.

Both simulator and app model incorporated the mistaken understanding of the role of the CHECK STOPS button. With both, the TMS accepted the changed headcode when the HOME button was pressed, which was not the case with the real train.

Human factors failure

It gets worse. According to RAIB, between 2014 and 2016 Hitachi commissioned a specialist to review the design from a human factors and ergonomics perspective. This work included an extensive review of the TMS. 'Many comments were made on how the TMS screens could be improved to better match users' expectations' notes RAIB, adding 'however, none of the comments related to any possible confusion or ambiguity associated with the process for entering a headcode'. But as an informed source summed it up: 'A user interface is like a joke. If you have to explain it, it's not that good'.

None of this, of course, excuses the driver's behaviour in dealing with the TMS with the train on the move – but it does explain it. And you may also wonder why such an obvious APCO trap and the importance of setting the ECS headcode was not briefed to drivers.

©2020 EngPro Solutions Ltd.

Scalded Cat

Another factor that caught this experienced driver out was the difference in performance between the Class 800 and the IC125 he had been used to driving. Different trains have different responses to the power controller. Class 55 Deltics, for example, were hair trigger. On wet days drivers had to be careful not to get wheel slip at the entrance to Gasworks Tunnel leaving King's Cross.

As a result of DfT's bonkers specification, the 800 Series trains are set to accelerate like a metro car from standstill. On only his third unaccompanied duty on a Class 800, the driver selected what he thought was a low power setting when moving off to follow the IC125 after the brief stop. And this is a driver of nearly 35 years' experience.

In fact, he selected about 20% tractive effort, which was enough to accelerate the train to 15mph in 27 seconds. With an IC125, a similar power application would result in half the acceleration rate. On top of that, RAIB estimated that where it would take around eight seconds between the controller being opened and an IC125 starting to move, the response of the Class 800 is about half that time. Overall, an IC125 would have reached around 7mph in the 27 seconds. This would probably have given the driver time to look up and see the approaching rear of the train in front.

Configuration

Apart from the flawed TMS ergonomics, a key lesson is the importance of configuration control in this new generation of software enabled trains. Like Windows or Apple's iOS, traction software is now continuously evolving. Periodic software 'drops' will continue throughout a fleet's service life. Keeping track of the software status is one thing, but configuration control also has to include driver training in the loop.

In the computer world, Windows 10 users have come to dread the regular upgrades because they don't know what adverse effect the latest update will bring. In one of its 'learning points' from the accident, RAIB reminds train operating companies of the importance of briefing their drivers about engineering changes made to the trains that they operate.

Back home after repair: driving vehicle of No 800109 on 27 October 2020 following delivery to Hitachi's Newton Aycliffe factory in County Durham. James Garthwaite

©2020 EngPro Solutions Ltd.