

A Brief Quest for Lesser-Spotted News Articles in Dependability



In this article, Wendy Owen explores and draws insights from a range of recent newsworthy articles from the rail, aviation, communications and marine sectors.

If you keep up with engineering news, rarely a week goes by when one might spot or hear of an article in the news – online, on TV or radio, in a newspaper, through networks – that has safety and/or operability implications. We see them but, unless we have some direct or vague involvement, we often don't have time to dig further and just skim over them. I started paying more attention to news articles for a few months, purely to see what appeared and to ponder on them rather than skim over them.

One thing that has made me ponder over the last few years reading various articles is how on Earth certain untoward scenarios that occurred during operations were seemingly missed or omitted, presumably during the design stage. Such scenarios being not necessarily hazardous, but yet also seemingly highly unlikely to occur if good processes had been implemented during the design phase. Perhaps one might expect such anomalies to occur with very novel or very complex systems, but these are often not the subject of the reporting. In highly regulated sectors, safety cases are common, but dependability cases – in their own right – are not as common as one might expect. Even the word dependability tends to still be restricted to certain sectors. In this article, I am talking about dependability (with an overlay of resilience). You'd think dependability would be having a field day with current

advances in technology, with enthusiastic Reliability, Availability, Maintainability (RAM) engineers keenly demonstrating the great characteristics of various new-fangled innovative systems. But rarely does one see job adverts for RAM engineers nowadays, and reliability engineers apparently keep databanks up and running.

From what I've been seeing in the news, something is not right down in the reliability woods and beta factor coppices. I began to postulate what has been happening? In the case of highly regulated sectors, I wondered if in some cases HAZOPs have been morphing into HAZIDs and thus losing their OPerability quotient, or if the guidewords had not been sufficiently diverse to pick up future reliability issues, or if they had become more like tick-box exercises rather than exercises in broad and innovative thinking. Was any RAM analysis actually being conducted? I aimed to pay a bit more attention to news feeds and seek out articles where the OP, or perhaps a RAM or Human Factors (HF) analysis, may have helped prevent large outages, shocks, or accidents.

Over the course of a few months the following interesting examples appeared. I make no claim to knowing if any of the associated companies or projects here did a dependability, operability, HF or resilience analysis, these are purely my own observations as a third party.

Titan Submersible Implosion (June 2023)

I feel reasonably SQEP to talk about this one as I've worked on similar submersibles in the distant past, and a former manager was an advisor to the Kursk submarine accident. Consequently, when this happened, I was glued to the ongoing newsreels, mostly thinking if it hasn't imploded by now, it will do shortly, and commented as such to the UK head of naval safety, who was obviously keeping largely quiet on the matter until the situation was confirmed. In the end, the submersible clearly wasn't structurally reliable for its intended scope of operations, ergo neither was it safe. The investigation is ongoing at time of writing, but it has become evident that the company had not sought certification for the vessel, arguing that *"Bringing an outside entity up to speed on every innovation before it is put into real-world testing is anathema to rapid innovation"*[1], a subject in itself.



Titan steering control –
Logitech F710



Titan end cap recovered

What I want to tease out here is that in this case it became obvious that 'successful' operations and the purported reliability of the missions to date (not many) had been prioritised over real design safety margins, and by a long chalk. The concepts of safety margins and structural reliability clearly went out the window - or weren't even in its frame. Issues were raised by the design team but ignored. And it hadn't been rigorously tested before going into operation.

The message here is just because it appears reliable, dependable, or even a fantastic innovation, doesn't mean it's safe, and it also doesn't mean you should ignore implementing a comprehensive reliability testing plan or creating a DRACAS.

Chaos on Sydney Trains (July 2023)

I have worked on a few Australian rail projects but not in Sydney, so of course this one caught my eye. Their metro is “fully automated” with Communications-Based Train Control (CBTC) signalling technology. A similar set-up can be found in Copenhagen, Milan and a few other places. This metro began operation in 2019 and carries about 20 million passengers annually. At time of writing, it has 13 stations and 22 trains with 22 miles of track, and over 30 stations under construction with aspirations of 70 miles of track. This metro proved very robust one day in July 2023 whilst the rest of the Sydney train network entered, well, a state of chaos. Even, a highly predictable state of chaos.



Ornate Sydney Station departures board (now in a museum)

"Vast swathes of Sydney's train network came to a standstill in the middle of the rush hour on Thursday because a single member of staff called in sick. Commuters were stranded on trains and on platforms across the city as the issue, which ... had cascading effects on much of the rail network. ... "Sydney Trains had late notice of resourcing issues this afternoon at the Rail Operations Centre. As a result, the continuity of the operations plan was impacted,"...."The resourcing issue involved highly specialised roles and the incident will be reviewed."..... By late afternoon, another signaller had come on shift. However, by that time, chaos has spread to trains throughout Sydney.... Commuters were given conflicting information and drivers had little idea how long the disruption would last. Enormous queues were seen at major hubs Replacement buses had to be scrambled to take passengers home.... every train line suffered some form of delay. Only the Sydney Metro, which is run completely independently from the Sydney Trains network, was unaffected. Passengers were left bemused as to why there was no backup in case just a single person couldn't come into work. One commuter said "It's absolutely crazy. How can one person calling in sick make such a massive difference?"[2].

And they were right. It is absolutely crazy that one person calling in sick could disrupt the journeys of tens of thousands or millions of people.

Maybe operability and human factors were considered in the course of design and planning, and this was just a case of 'bad luck' but, having spent a few years working for a signalling supplier/manufacturer, this particular event was akin to the loss of a critical path in project management or a single point failure in a physical system resulting in a high consequence event. It 'screams' of a dire lack of Human Factors Integration (HFI). Clearly, one member of staff being unavailable should not result in major signalling system downtime or major disruption on mainlines. This issue should have been picked up pre-commissioning.

The concept of “failure” applies as much to humans as to systems. If you're looking at

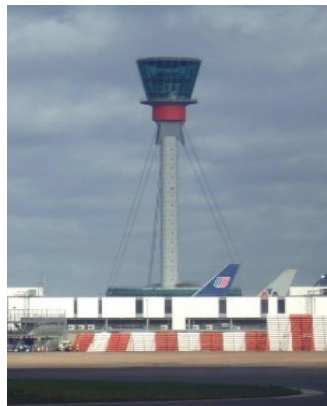
transport systems involving high interaction with the general public, or if throughput of people is critical, or if you need continuity of operators to operate (as in this case), then humans are integral and critical to successful (and reliable) operations and system availability.

The main messages from this one are please don't forget about the humans, including sick ones, and don't forget to do operability and HFI studies. My own experience says maintainability assessments can also reveal similar gaps, so don't forget those either.

NATS Goes Haywire (August 2023)

Having very briefly worked on NATS during a major upgrade about 20 years ago, I was surprised to read this article [3]. However, I won't delve deeper into this one as no doubt it has been so high profile that there will be lots of people here writing about it who know a lot more about the systems than me. Although it appears that the system had the correct and safe reaction in the circumstances i.e., it shut down, externally it appears as an operability issue – the transport system ground to a halt (pardon pun), similar to the Sydney trains.

It's a good example of where there is a question about how much unavailability or downtime are the travelling public prepared to accept, and how is that balanced against safety or company reputation?



Heathrow traffic control tower

Comms Chaos Down Under (Nov 2023)

Even worse than the train network chaos back in July, on 8th November a report came on the news about "Optus outage: Millions affected by Australian network issues" [4].

On closer inspection, *"The failure caused transport delays, cut hospital phone lines, and shut down payment systems... more than 10 million people and thousands of businesses were affected... Services were restored after around 12 hours of disruption....there was no evidence of a cyber-attack. The firm blamed a "technical network fault" and said more time would be needed to investigate the root cause.... People across Australia were unable to call emergency services and critical helpline numbers. Train services in the state of Victoria were also temporarily crippled."*



This serves as an excellent example of how widespread the impacts can be across industry and everyday lives of "uptime"/"downtime" and safety from a single source of failure in national critical infrastructure.

We can hope that the communications network concerned are having a serious investigation of the cause and the subsequent chain of events and are planning to employ a large department of systems assurance engineers.

End Notes

In my quest for articles involving dependability, I have observed that modern society is becoming more dependent on technology, more dependent on people doing the right things, and, mostly, more dependent on identifying potential problems at design stage. Any systems affecting critical infrastructure are of particular importance.

Many industrial sectors need good dependability cases (and peer reviews thereof) more than ever, as incidents resulting in system downtime increasingly have major impact on business continuity and/or society. Next time you spot potential for a critical system or business going 'out of action', remember the OP bit.

Sometimes there's also safety implications – as has always been the case – but, without a formal dependability management regime/framework in place alongside the safety and human factors i.e. an integrated RAMS and HFI approach, together with management or duty holders who genuinely support such efforts, reliability and safety still have the means to tread a delicate, or even difficult, balance.

References

- [1] <https://www.theguardian.com/world/2023/jun/21/titanic-submersible-documents-reveal-multiple-concerns-raised-over-safety-of-vessel>, accessed Dec 2023.
- [2] <https://www.news.com.au/national/nsw-act/news/single-sick-staff-member-sends-sydney-trains-network-into-chaos/news-story/0c28a932125aa79e2795f028155d5e7a>, accessed Dec 2023
- [3] <https://www.bbc.co.uk/news/uk-66685349>, accessed Dec 2023.
- [4] <https://www.bbc.co.uk/news/world-australia-67340901>, accessed Dec 2023.

Image attribution:

Titan controller: https://en.m.wikipedia.org/wiki/File:Logitech_F710.jpg CC BY-SA 3.0

Titan endcap removal: https://en.wikipedia.org/wiki/Titan_submersible_implosion#/media/File:231001-G-G0000-1001.jpg public domain

Sydney departures board: https://en.m.wikipedia.org/wiki/File:Central_Station_indicator_board.jpg CC BY-SA 3.0

Heathrow tower: https://en.m.wikipedia.org/wiki/File:Heathrow_Traffic_Control_Tower_-_geograph.org.uk_-_144749.jpg, CC BY-SA 2.0

Triple zero: Photo 65600746 © Ymgerman | Dreamstime.com

Wendy Owen

Wendy has 35 years' experience in systems assurance across a wide range of highly regulated industries covering energy, defence, transport and process sectors. Her career has largely been in engineering consultancy, also with time in product development, research and regulatory. She is a Fellow of WES and the Safety & Reliability Society, and within the SCSC she is a task lead in SiSWG, a member of the Steering Group and lead for the Diversity Equity and Inclusion (DEI) initiative. She is currently freelance.

The author retains copyright of this article.