The Institution of Railway Signal Engineers Inc

Australasian Section Incorporated

RAMS – is that when you have more than one sheep?

Peter Burns
MBA BAppSci CPEng MIEAust MIRSE
PYB Consulting Pty Ltd

1.1.1.1.1 SUMMARY

RAMS analysis and the setting of RAMS requirements (often expressed as single indices) are becoming common features of rail signalling projects.

But attempts to outsource RAMS objectives by attaching them as simple deliverables in project contracts often fail. This paper explores some of the reasons why this is so.

The paper takes a qualitative look at examples and processes of requirements analysis and requirements setting, particularly at key interfaces important to RAMS. These include:

- Interfaces with the rail environment and the world at large;
- Interfaces between signalling systems;
- Maintenance Policies and strategies;

It will be seen that the achievement of RAMS outcomes inherently involves alignment between many parties. Products do not stand alone; they are part of human centred systems. Success depends on openness by organisations and access to good engineering knowledge – these being the oxygen on which RAMS depend.

2 INTRODUCTION

As railway signal engineers today, we are fortunate to be living in an age when our industry is in resurgence.

As rail reinvents itself for the twenty first century, Signalling Engineering needs to move into the twenty first century also. I reflect that there are those who wear as a badge of honour the image of Signalling as a "Black Art" (as opposed, perhaps, to being a proper branch of Engineering).

The traditional method for developing signal principles (well tried for over a century) can be summarised as:

- start with a safety management system;
- wait for an accident to happen;
- do an investigation to determine what went wrong;
- change whatever caused the accident to prevent the same accident happening again;

This method is what Stephen Barlay[i] calls the "Tombstone Technology" approach. Historically it has been a common approach in many industries. To apply it, you just have to remember all the accidents and what you did to prevent re-occurrence of each one. A solid engineering foundation is not necessarily required. As each rail jurisdiction experiences its own unique set of accidents, each builds its safety systems on its own post-accident learnings, and the systems across jurisdictions are all different. The result can be a quirky patchwork.

It is even possible to have the interesting situation where a single measure mandated for safety in one jurisdiction can be prohibited due to safety concerns in the jurisdiction next door.

If this sounds familiar, it is certainly not new. A look through the IRSE archive reveals a paper A.F. Bound presented in 1915 promoting the use of a new-fangled device called a track circuit. In the discussion which followed, the following (perhaps tongue in cheek) comment was recorded from H. G. Brown:

> "*Mr Bound's suggestions tend to destroy one of the most interesting features of the art of signalling, and that is its infinite variety – the fact that exactly the same conditions are never treated twice in the same way. This lack of coordination, whilst inexcusable, creates great interest.*
>
> *"From the discussion of this paper it would appear that there is a decided feeling of antagonism between the adherents of Lock and Block and Track Circuiting. Those whose experience has been limited to one seem to have but little appreciation of the other*."

Such a comment, with technologies slightly adjusted, would not seem out of place in any IRSE meeting today. Not much has changed in the intervening 100 years.

The tombstone technology approach does not provide very good tools for dealing with the introduction of new technology. How do we know whether our new technology is safe before accidents have had time to occur?

Fortunately, the modern age provides modern alternatives for systems development. This is RAMS analysis (Reliability Availability Maintainability Safety), the topic for today.

Most of us are quite familiar with RAMS. There are a number of standards, and there is a common approach:

- SIL-4 equipment is called up for every vital signalling application, and

- clauses in standard project contracts call up RAMS objectives for suppliers to meet.

Job done?

The problem is that the RAMS analysis approach is not really a bolt-on to the traditional Tombstone Technology approach, it is actually an alternate paradigm. It is a much more powerful paradigm because it can manage migration to new technologies and does not involve waiting for the accidents to happen before the causes are addressed.

It also underpins the development of common, technically defendable, standards.

Unlike the more traditional approaches, the RAMS analysis approach requires a much more solid accessible base of quality engineering data on seemingly relatively mundane matters. Modelling mechanisms for equipment failure (right and wrong side) becomes important, as does understanding the failure rates for each one. This is the FMECA (Failure Modes Effects and Criticality Analysis).

Beyond the FMECA, there are other items also needed to obtain the full systems models for carrying out the RAMS analysis.

The remainder of this paper will look at a sample of some of those "other things" which are needed for a proper RAMS analysis and some pitfalls. The information needed comes from multiple sources, many outside the control of the typical equipment manufacturer. Much of the information needed is from traditionally secretive customer organisations; much else is generic and fertile ground for technical research which could be productively promoted by this Institution.

3 ALASKA AIRLINES FLIGHT 261

3.1 The incident

This example is drawn from Chapter 2 of Sidney Dekker's excellent book "Drift into Failure" which I recommend you all read to get a much fuller account of this incident than I can provide here.

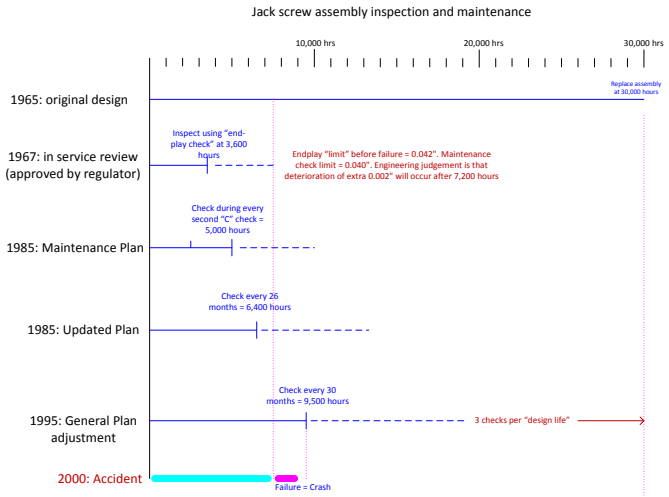
Quoting[ii]: "In the early afternoon of January 31 2000, Alaska Airlines flight 261, a McDonnell Douglas MD-80 took off from Puerto Vallarta in Mexico, bound for Seattle ... "

Sometime into the flight, the jackscrew and nut assembly required to operate the plane's horizontal stabilizer became stuck due to thread-wear. This failure meant that the aircraft's horizontal stabilizer could no longer be operated by the pilot. With no horizontal stabilizer, the aircraft essentially became uncontrollable. The aircraft crashed in spite of the best efforts of one of the most skilful pilots you're likely to read about. All on board died.

Sidney Dekker then takes us through the long chain of events leading up to the crash. This chain extended over a period of 35 years between when the first DC-9 was certified and 2000 when the crash happened. It looked at the original design and tracked all the changes to maintenance policy over the period.

The crash was caused by failure to replace a life-expired jackscrew and nut assembly prior to its failure in service.

The following diagram summarises the evolution of the maintenance policy for the jackscrew assembly over the period.



Initially, with as much lubrication of the jackscrew assembly as it originally recommended, Douglas thought it had no reason to worry about thread wear. So, before 1967, the manufacturer provided or recommended no check of the wear of the jackscrew assembly. The trim system was supposed to accumulate 30,000 flight hours before it would need replacement.

But operational experience revealed a different picture. After only a year of DC-9 flying, Douglas received reports of thread wear significantly in excess of what had been predicted.

In response, the manufacturer recommended that operators perform a so called end-play check of the jackscrew assembly at every maintenance C check, or every 3,600 hours. This decision reflected a combination of an appreciation of the criticality of this component to the operation of the aircraft as well as the wear being more than anticipated.

From 1985 onwards, coinciding with the deregulation of the airline industry, end-play checks at Alaska Airline became subject to the same kind of drift as the lubrication intervals. In 1985, end-play checks were scheduled for every other C check, as the required C checks came in every 2,500 hours, the check occurred every 5,000 hours.

By 1988, C-Check intervals themselves were extended to 13 months. End-play checks were thus performed every 26 months, or about 6,400 hours.

In 1996, C-check intervals were extended once again, this time to 15 months. This stretched the flight hours between end-play checks to about 9,500 hours.

The last endplay check of the accident airplane was conducted at the airline maintenance facility in 1997.

At that time play between the nut and screw was found to be exactly at the allowable limit of 0.040 inches. What to do? The maintenance facility did not hold the part, so would have had to order it in.

So, the aircraft was released: Sidney Dekker records the maintenance release as logged: '"departed 0300 local time. So far so good" the graveyard shift turnover plan noted'.

Three years later, the plane crashed.

Although this incident did not occur in the rail industry there are clear lessons we can draw from it.

3.2 Substantive lessons

In the late 1980s, I was Maintenance Support Engineer in Melbourne. The same trends affecting aircraft in the US were felt in Signal Maintenance here. One view, believing equipment to be generally over-maintained, was that we should adopt a policy of simply increasing maintenance intervals and see what happened. The Air Alaska incident shows the other end of that type of process.

There was an alternate competing philosophy. This philosophy said that we should collect data concerning all known failure modes for a piece of equipment or system, build a failure model (or models) for that equipment or system, then use the model in conjunction with engineering judgement to establish a recommended maintenance plan, inclusive of a margin for maintenance cycles being late or missed. This can then be compared with existing maintenance practice and the differences analysed. You will be familiar with the modelling process as a FMECA (Failure Modes Effects and Criticality Analysis). With a few additional processes added, you have a RAMS analysis.

3.3 Lessons regarding data

As part of original regulatory certification of the DC 9, it is clear that some form of FMECA was undertaken. 40 years later, the work was still available within relevant US government agencies for Sidney Dekker to inspect and comment on. In this respect, the aircraft Maintenance Support Engineer was probably slightly better off than the typical Rail Signalling Maintenance Support Engineer in Australia. There is no regulatory public agency here in Australia which requires rail FMECAs (or Quantified Safety Cases for that matter) to be made available and published in a place accessible by Maintenance Support Engineers.

Sidney Dekker discusses how the original engineering work towards regulatory certification contained a lot of items determined by “engineering judgement”. That is to say the hard data called for by the model did not exist. We live in an imperfect world now as we did then. But the “engineering judgement” in this case turned out to be right. With knowledge of the normal allowances made in converting engineering wear calculation into maintenance policy, it is possible to use the maintenance plan put out in 1967 to correctly predict the accident in 2000.

The maintenance planners for Air Alaska either:

- did not make use of the information produced in 1967; or
- did not believe the conclusions were correct

Compared to us now in the Rail Industry they did have the major advantage that the engineering data and calculations did exist in a publicly accessible place for those who wanted to look. The same cannot be said for maintenance planning engineers in signalling in Australia today.

But Sidney was also right - uncertainty is what creates risk. In this case, the risk is that the engineering judgement was wrong and the maintenance regime was insufficient to prevent an accident. The only way to reduce that risk item in the safety case is to get more and better data.

Thus, data lies at the core of safety.

4 TRI-COLOUR SIGNALS

In railway signalling, one recent example of new technology being introduced are LED signals. These are replacing traditional incandescent signals. Incandescent signals are well understood and the literature mature. Failure modes, equipment life, maintenance plans, are quite well established. The same cannot be said for LEDs

With the introduction of LED signals, the immediate tasks for Rail Authorities have been:

- Type approval – specify the methods for safe use of the new product in your own jurisdiction;
- Maintenance planning – establish appropriate maintenance policy for the LEDs purchased to ensure RAMS objectives are met.

A safety case needs to be developed, maintenance strategies (different from those appropriate for LED signals) developed in conjointly with selecting the configuration of the LED signal modules to be used. And there is also a 6 month in service trial.

4.1 Safety at interfaces

Mid last decade, a number of tri-colour LED signals were type approved for operation in Victoria. These signal modules were offered as SIL-4 products to be interfaced with SIL-4 interlockings. Two incidents which occurred in late 2006 illustrate why simply connecting two SIL-4 products together without adequately analysing the interface assumptions made by the safety case of each, can give a less than SIL-4 outcome.

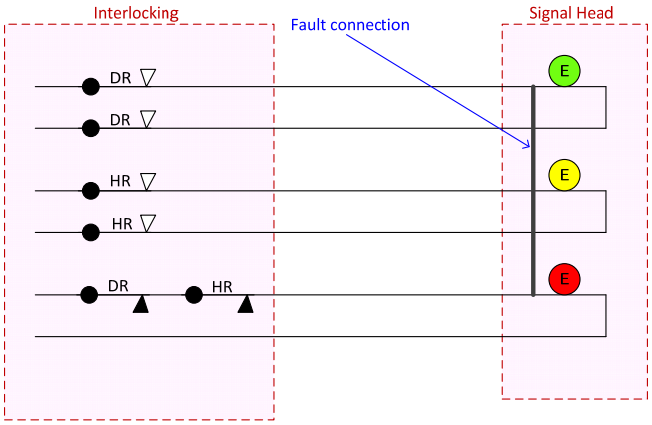
In this case the LED modules were of a 4 – wire type with a common negative return.

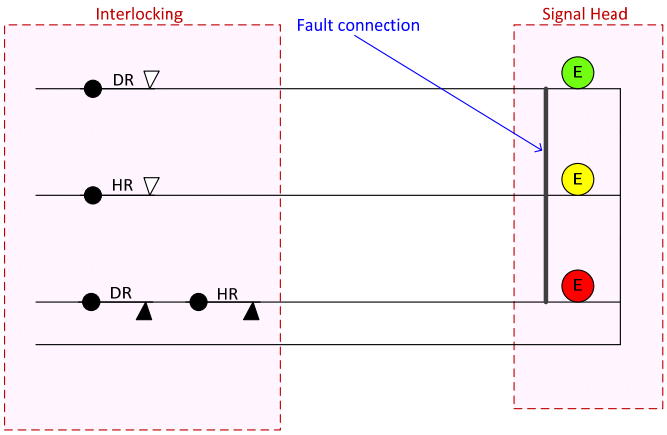
The potential safety risk in this approach is that a single short in cable or signal head (earth fault or simple short) can cause illumination of a wrong aspect. This is a failure mode well known and understood by interlocking designers.

In relay interlockings, the risk is dealt with by using a 6-wire lamp circuit and:

- Double cutting the lamp supplies so that two supporting (hence much less likely) faults are required to cause a false illumination; or
- Providing a separate isolation transformer (Location Case mounted) for each lamp, again preventing a single fault from causing a false illumination.

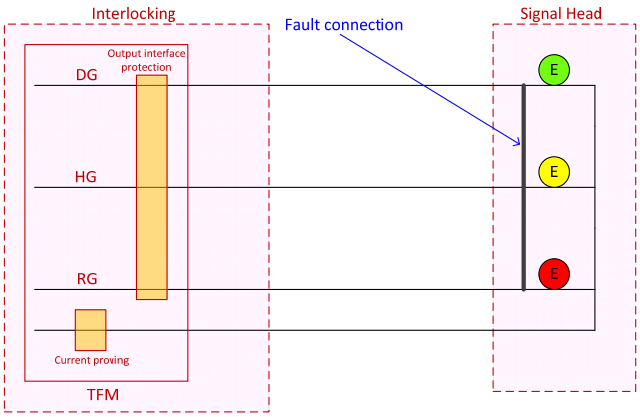
The following diagram illustrates the typical LED circuit:





In more modern SSI, the Trackside Functional Module (TFM) has a single negative rail with current proving provision. Thus the techniques used in traditional relay interlockings are not effective in preventing false illumination in TFMs.

Instead, the TFM provides a separate protection layer called an “Output Interface” for each module. The task of the output interface is to detect, on any un-driven output, any stray voltage present which may indicate a false illumination in a signal. If such voltage is detected, all power to all module outputs is shut down, thus preventing a false aspect from being displayed.



The new 4-wire LED module, based on its design which featured a common return wire, could be certified safe to use in SSI applications where the TFM utilises a common return with output interface protection. SIL-4 could be established for this quite common application.

The problem occurred where the 4-wire LED module was utilised in a traditional relay interlocking which clearly does not have an output interface shutdown mechanism.

The question which arises is how, as an engineer, I can be aware of the interfacing issues with a product such as this LED tri-colour module. The typical “6 month type approval trial” is unlikely to uncover a safety issue even at a SIL-2 challenge level, leave aside SIL-4.

One answer is to inspect the FMECAs associated with the safety case for the LED signals in association with the safety cases for (a) SSIs and (b) relay interlockings. These last two perhaps should be done by the designers and safety assurance analysts for the LED module manufacturers.

The “room full of records” which makes up the SSI safety case is over 25 years old now. How does an engineer designing LED signals go about inspecting that safety case data? One begins to feel envious for Sidney Dekker who was able to access 40 year old safety case data for a DC-9 aircraft.

In the case of the LED signals, one manufacturer estimate made prior to type approval was for a single short circuit (earth fault) event in the signal head. That estimate was that such failures are “extremely rare”.

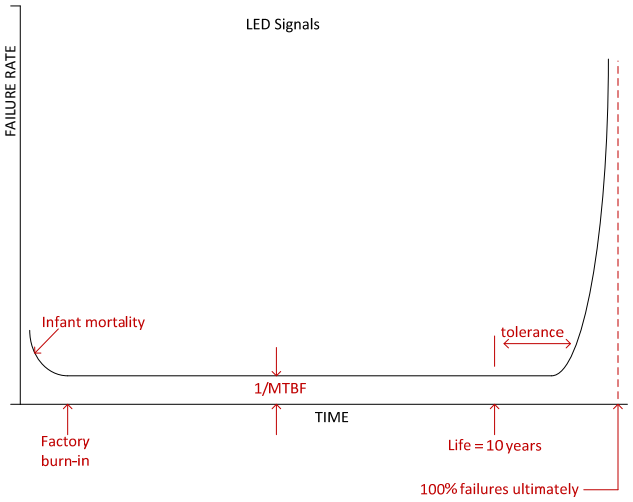
Whether this estimate was consistent with the observed failure rate (2 failure events within the space of 6 months) is doubtful, yet important. An unbiased estimate (via appropriate study), even now, would be a valuable contribution to engineering knowledge in our discipline.

4.2 Maintenance strategy for availability

Leaving aside the “S” portion of RAMS, maintenance strategy is quite an important consideration for LED signals RAMS analysis. One significant benefit quoted for switching to LED Signals is the reduced requirement to maintain.

But the contribution which maintenance policy (set by the Infrastructure Manager, not the manufacturer) makes to the RAMS outcome makes it difficult for a supplier to make commitments on particular outcomes in isolation.

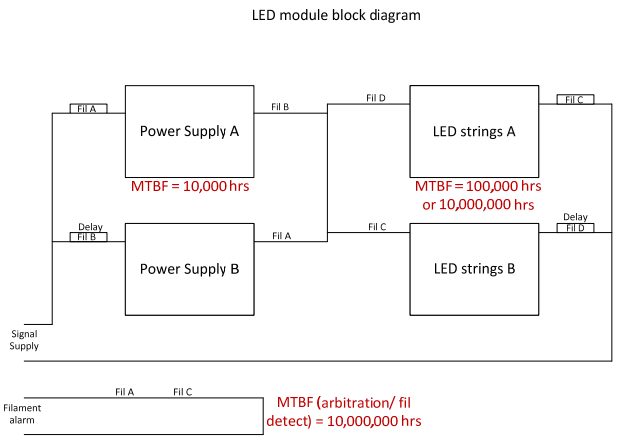
Typically the data available from manufacturers for LED signals is “Length of life” data. LEDs fail by wearing out (similar to bearings). The following diagram illustrates the failure pattern typical:



For a signal in mid-life, the MTBF (Mean Time Between Failure), which determines the practical failure rate, will typically be very much higher than the expected life figure quoted by the manufacturer.

A common target strategy is to carry out a planned replacement just before the end of life failures commence (the same maintenance strategy used by motor mechanics for bearings on cars). Using this strategy, the rate of lamp-out events depends entirely on the MTBF figure for a mid-life LED – small but finite.

The system can be improved by borrowing a concept from the incandescent days and implementing the equivalent of a first filament failure alarm. There are a number of ways of implementing this, of which the following is one:



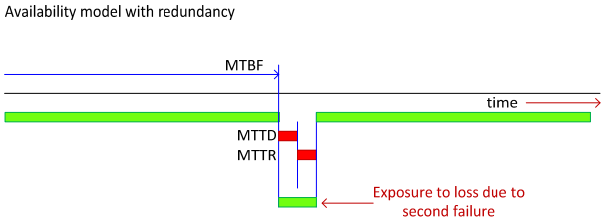
In this case, I have assigned some reliability figures for illustrative purposes only (those in need of such numbers need better sources). MTBF of the LED subsystem depends critically on the maintenance policy (replace before “end of minimum life” gives a very much better figure than “replace on failure”), and also displays measurable degradation as end of life approaches (allowing a condition monitoring approach to be potentially feasible).

The model shows that the least reliable component is the power supply. Maybe an alternate design would duplicate this and leave just a single LED subsystem.

There is a “first system failure” detection output provided. This requires supporting infrastructure to get any alarm (or analogue measure) back to a responsible maintainer. Is there a benefit in providing this infrastructure? This is a strategic decision for the Infrastructure Manager.

Given the costs associated with signals, masts, ladders and landings (some quite effective maintenance strategies do away with the need for these), and lamp out incidents (operationally), there would seem to be fertile ground for cost-saving research in this space.

In the configuration as shown in the diagram, lamp out risk depends on mid-life MTBF and MTTR based on a reliability model. The following diagram illustrates the failure scenario:



Mean time to detect (MTTD) is dependent on whether alarm infrastructure is installed, or whether reliance is placed on periodic maintenance inspections. Mean time to repair (MTTR) is set by the maintenance policy. The policy could involve a planned response to an alarm (whether within one hour or a week), or may be a cyclic planned activity (monthly or annual inspections). The appropriate periodicity depends critically on the MTBF figures for the sub-systems within the units.

For a dual filament arrangement, the need for a sub-hour MTTR is eliminated (since the first failure does not affect train running). But what should MTTR be to best balance cost and availability?

One possibility is to install a first filament failure detection similar to the SSI method, then on an annual basis go around in a high-rail cherry picker with power off replacing all alarmed signals. This could have the benefit of avoiding the need for ladders and landings on signals if the availability figures from working that way can be high enough.

With only length of life data available from manufacturer, clearly I need more data to determine whether some variant of my strategy can offer an economic (and reliability) benefit compared to a more traditional policy.

5 THE FIXED TRAINSTOP

One topical case for the safety of equipment in the context of detection and repair times relates to the case of the fixed trainstop.

You may recall that the IRSE recently inspected an installation at South Morang in Victoria with some of these.

The safety implications of a fixed trainstop are amply demonstrated by the incident at Broadmeadows in 2003 (8 people injured) where a terminating suburban train ran away and collided with a stationary train at Spencer St in circumstances where a fixed trainstop which could have stopped the train at Broadmeadows was not in place when needed.

The failure model is similar to that for the dual filament lamp but now with a safety outcome and expected frequency of occurrence quite different. The configuration of and maintenance policy for fixed trainstops changed following the incident at Broadmeadows.

Prior to Broadmeadows, a fixed trainstop was a fixed solid piece of metal. Maintenance policy was:

- The absence or presence of the trainstop was detected by periodic inspection (by track inspector and signal maintainer); interval unknown.
- Where fixed trainstop was absent or out of position, signal maintainer would replace it when notified (estimated within 1 week).

Post Broadmeadows, fixed trainstops were altered to be conventional trainstop mechanisms, continuously detected and interlocked with signalling. Maintenance policy is:

- The detection of the trainstop is via the signalling. Any trainstop out of adjustment will put signals to stop and stop trains;
- Repair of fixed trainstops is within 1 hour (or the typical signal failure response time for the maintenance organisation)

To compare the two approaches, the availability model is the same as that for the dual filament lamp presented in the previous section. For the safety incident to occur, the trainstop must be missing at the time the train challenges it.

Thus we need to understand the frequency with which existing fixed trainstops are challenged by trains. This is yet another potentially fertile topic for study by a graduate student. Based on known incidents, a lower bound (quite conservative estimate) per trainstop of the order of one incident per 1,000,000 hours may be appropriate.

If maintenance practice results in the loss of a trainstop being detected and trainstop restored within 6 weeks of its removal (the normal signal maintenance cycle), mean time between incidents is approximately 1 billion hours, well in excess of SIL-4 requirements. Even an annual inspection regime would meet the requirements of SIL-4.

I can understand the Infrastructure Manager's frustration in this case that perhaps not even an annual inspection was being effective.

With the revised regime, mean time between unsafe incidents runs out to 114 million years. Whilst this by itself could be seen as a good result, it comes at the cost of putting a signal at stop during a right-side failure. This is operationally disruptive and not a risk free process, though the reason why is the topic for another paper.

The net result of the new policy has quite possibly been a reduction in safety rather than an improvement.

With this example we see a classic case of Tombstone Technology in action.

That there is a better way (the RAMS approach with an interdisciplinary team) has been clear for many years.

6 CLAMP LOCKS AT STH KENSINGTON

6.1 The investigation

In the 1990s, a new SSI interlocking was installed at South Kensington (Melbourne). Along with the interlocking, a lot of field equipment was renewed, including the changeout of some old style point machines with then modern Victorian Clamp Lock Point Mechanisms.

Soon after commissioning, the rate of point failures at South Kensington started going through the roof. I was asked to investigate and find out why.

Finding good design data for this home-grown point mechanism was quite a challenge. The mechanical design drawings were marked with the occasional tolerance figure, but no information was available as to why a particular tolerance number was important or even whether it was important.

The original design drawings were not accompanied by a design report outlining the reasons for design decisions made; and of course in those days there was no safety case documentation accessible.

So I employed a cabinetmaker to construct a scale model in wood of the important structural components of the device and put it through its paces.

What I discovered was that there was a tolerance of 10mm on the relative height of point blade and stack rail which, when exceeded, caused the clamp lock mechanism to mechanically lock up. Interestingly, this was exactly the type of failure which was being reported from the field at the time.

The standard remedy – add graphite – had been carried after each failure. Now we knew why it had not worked.

Here we had a classic Edward Deming situation:

- The equipment causing the failures was under the control of another discipline (track maintenance), hence there was a requirement for an interdisciplinary team to fix the problem;
- The track maintainers were maintaining the relevant dimension to a tolerance of 25mm, though the failure tolerance was 10mm. This is what needed to be fixed.
- The track formation itself was more than a little bit unstable, being built on top of a foundation material called "Coode Island Silt", a material apparently impossible to fully stabilize.

It was really interesting work. I wrote up a technical paper outlining the problem. Where did that report go? In those days, it went into the drawer of the departmental manager. Then, when he/she retired, was promoted, or simply ran out of space, it was most likely transfered to the round filing tray.

Authors were not permitted to put their own names on work which they did. So what do you suppose the chances were of such a piece of work finding its way into an externally available technical paper, or being presented to a body like the IRSE?

For some other engineering and scientific disciplines, such publication is pretty routine. For Railway Signalling, locating that paper now is a matter of knowing which landfill site to excavate.

The question for us is: what happens to technical papers like this in our industry today? Where would such work be published?

At the start of this paper we discussed the case of the Alaskan Airlines crash. We saw that Sidney Dekker was able to publish a blow by blow account of how it happened because the relevant records, including technical reports, still existed (40 years after the original work was done) and available to be read.

We showed how such technical information was vital for a maintenance support engineer (in his/her RAMS analysis) for making safety critical decisions on maintenance strategy and maintenance planning.

That is how it works in the aircraft industry. How does it work for us?

With this example we come full circle.

6.2 Why should a body like the IRSE be concerned about Engineering knowledge?

Most Engineers today are familiar with the case law which sits behind the modern "So far as is reasonably practicable" approach to rail safety.

There is a parallel stream, also grounded in Negligence case law, which deals with the responsibility of the expert in meeting his/her responsibilities in exercising "reasonable skill and care". The material quoted involves financial auditors, but may have some relevance to us today[iii] .

A question which must therefore be asked is: will an audit conducted in accordance with the accounting profession's current auditing standards and practice statements satisfy the test of reasonable care and skill?

Sheppard J in Employees Corporate Investments Pty Ltd v. Cameron[iv] stated that:

> *" …although the extent of an auditor's obligation is ultimately a matter for the Court (Florida Hotels Ltd v. Mayo[v]) the court will nevertheless take into account evidence given by persons experienced in the particular profession involved as to standards which are considered appropriate within a profession."*

This view is supported by the United States case of "Escott v. Bar Chris Corporation[vi] where it was stated that

> *" … accountants should not be held to a higher standard than that recognised in their profession".*

However, it does need to be acknowledged that, as stated in Continental Vending US v. Simon[vii], whilst compliance with the auditing standards may be very persuasive, it is not necessarily conclusive evidence of exhibiting reasonable care and skill if those standards are inadequate. In that case the judge discounted the evidence of the expert witnesses on the basis that the critical test was whether the accounts were presented fairly, rather than whether the defendants had acted in good faith. Also in the United States case of Hochfelder v. Ernst & Ernst[viii] the Judge stated that:

> *" … we are not constrained to accept faulty standards of practice otherwise generally accepted in an industry or profession".*

As a result, there is a need for the profession to ensure that auditing standards are "up-to-date" and have taken into account changing circumstances and technology.

The discussion quoted here about the need for a profession (any profession) to have standards that have a firm foundation and able to cope with changing technologies is relevant to Signal Engineers also.

6.3 Where do we go from here?

In the Alaska Airlines case discussed at the start, the question "what should they have done?" could be answered by pointing to the good technical work which had been done in 1967 and which was publicly available to the following generation of engineers. If only they had read it.

The safety of their travelling public depended on it.

For our profession it does us no favours if similar good technical work is not there and available to the profession to form a basis for our similar RAMS analyses. The safety of our travelling public also depends on it, as does the reliability (including the operational reliability) of our train system.

Within the Signalling fraternity, the non-analytical way of thinking which struck H. G. Brown as a problem back in 1915 remains too prevalent for us today.

But today with the advent of the Post Graduate Diploma and the Masters Degree (via Central Queensland University) the opportunities are there to initiate the technical studies into important topics and to have them published to the benefit of the profession as a whole.

Perhaps the time has come to ditch the "black art" reputation with its dogma and tombstone technology approach, and set about strengthening the technical foundations, do the studies, put the profession on a base sufficiently scientific to support quality RAMS analyses.

7 CONCLUSION

Unless we understand the reasons why things are done as they are, it is impossible to safely change the ways things are done.

Now, as we enter the twenty first century, the need for change is there as technology rapidly develops. For how much longer can the view be accepted without challenge that the best way to detect a fault in a piece of equipment is to set a signal to red and stop a train?

The ability to do better is there but it requires that:

- We understand our systems and the environments in which they operate, putting in place a solid foundation of technical knowledge; and
- System design, operational environment and maintenance strategy develop together towards common goals, recognising their mutual interdependence.

By embracing RAMS concepts, utilising calculated levels of redundancy, utilising condition monitoring, and doing the analyses, we can underpin a future where “fail safe” can increasingly be supplanted by “never fail” as a guiding principle.

Such a world would be safer (Glenfield and Craigieburn would not have occurred without signal failures) and maintenance costs could be less, not because we mindlessly increase maintenance intervals, but because we truly understand our systems and design them to be so.

PETER BURNS

After graduating in Applied Science (Electronics) from Melbourne University in 1981, he commenced working with Victorian Railways in Signal Design Department (started in “Level Crossings”).

He progressed through a number of roles (Signal Design, Test and Development, Maintenance Management). Completed MBA at Monash University in 1991. In 1994 he left the then PTC and moved to Sydney to work with GEC Alsthom.

As Senior Designer, he designed and checked large interlockings, trained staff, managed projects and developed products.

Returned to Melbourne to join the TMF project in 1999. His various Systems roles included a year in Denmark managing a TMS product release.

He is currently director of the small consultancy firm “PYB Consulting” and assists the Regional Rail Link Project package B amongst other things.

The Institution of Railway Signal Engineers Inc

Australasian Section Incorporated

Approval to Publish Technical Papers

I / We ……..

of Company (if applicable) ……..

hereby give permission to The Institution of Railway Signal Engineers Inc Australasian Section Incorporated to publish the Technical Paper titled:

Insert Title ……

To be presented at the IRSE Technical Meeting to be held at:

Location …… on Date …….....

In the following media:

Tick as appropriate

☐ Publish on the IRSE Australasian and international web sites or in the Proceedings

☐ Permission to allow recording/streaming of audio and/or video of the presentation and discussions

☐ Inclusion in a CD of past Convention Papers for sale by the IRSE

☐ Publish in the bound volume of the Convention Technical Papers (if provided).

Signed: ……

Date: ……

Please return this form when submitting the final version of the Technical Paper.

Approval to Publish Technical Papers

[i] Stephen Barlay; “The Final Call” (1990), Ch 2.

[ii] Drift into Failure, Sidney Dekker, 2011, Chapter 2

[iii] Baxt. Role of the Auditor, in Company and Securities Law Journal, April 1989.

[iv] (1977) 3 ACLR 120 at 131

[v] (1965) 113 CLR 588

[vi] (1968) 283 F.Supp. 643

[vii] (1969) 425 F. 2d 796

[viii] (1974) 503 F. 2d 1100