Rail's Particular Challenge with Resilience: Shifting from Controlled Complicatedness to Working with Complexity

Alexandra McGrath, MIRSE B.Eng(Elec) B.Comm, VicTrack

SUMMARY

The field of resilience engineering explores the mismatch between a system-as-designed and the actual system as it operates in the real world, in the presence of shocks, stresses and resource constraints.

At the core of resilience engineering is a philosophical difference from other types of engineering. Conventional engineering sees a technical system such as a railway as complicated, but ultimately controllable, fully modellable and predictable from the behaviour of its components. Resilience engineering has at its foundation complex systems thinking, which sees the system quite differently: a system is composed of technical and organisational parts and human or social agents which interface and interact with each other. System behaviour can be partly explained through interactions at the interfaces, resource flows, adaptive cycles and patterns that repeat across scale and time. The tools of a complex systems thinker or a resilience engineer are curiosity about contradictions, experimentation, feedback and targeting activity to intervene at the most appropriate point of an adaptive cycle - both the appropriate scale and the appropriate phase.

This paper gives an introduction to resilience engineering, a discussion of safety and the changing worldwide approach to safety management, an exploration of rail in general, with case studies from Victoria, Australia. A contrast will be drawn between a command and control perspective and a complex system adaptive cycle perspective, the limits of the command and control philosophy will be identified, and guidance and practical examples will be given of using the tools of resilience engineering to tackle complex system change safely.

1 RESILIENCE ENGINEERING: COMPLEX VS COMPLICATED

The tools of resilience engineering allow a complex-systems view of rail systems, in contrast to the complicated problem-solving approach of conventional engineering. Instead of focusing down-and-in, aggregating component models to assure inherent safety in a system-as-designed, resilience engineering seeks to understand interactions across boundaries and the mismatch between the system-as-designed and the real system.

1.1 Introduction to Resilience Engineering:

The field of resilience engineering seeks to understand the behaviour of complex human-technical systems under stress and crisis. The work in system safety of Hollnagel [1, 2], Dekker [3], Reason [4, 5] and others have argued that safety assurance at small scale (e.g. prevention of worksite accidents through administrative procedures and compliance) does not correspondingly reduce the probability or consequences of a system-wide catastrophic event, nor improve the protective capacity of that system to respond and recover from such an event. In fact, some data shows that a highly controlled and procedure-driven safety management system may actually increase the risk of a cascading castastrophe [3, 6].

For the purposes of this paper, the definition of resilience is drawn from Victoria's Critical Infrastructure Strategy:

> *"… THAT RESILIENCE OF INFRASTRUCTURE IS PROVIDED THROUGH GOOD DESIGN OF THE NETWORK AND SYSTEMS TO ENSURE IT HAS THE NECESSARY RESISTANCE, RELIABILITY AND REDUNDANCY, AND BY ESTABLISHING GOOD ORGANISATIONAL RESILIENCE TO PROVIDE THE ABILITY, CAPACITY AND CAPABILITY TO RESPOND AND RECOVER FROM DISRUPTIVE EVENTS. THE LATTER IS GAINED THROUGH BUSINESS OPERATIONS AND APPROPRIATE SUPPORT FOR BUSINESS CONTINUITY MANAGEMENT."*

The field of resilience engineering seeks to understand the things that mark the difference between a system that is vulnerable to a cascading catastrophe and one that has resilience. Researchers have recognised two things:

1) **A system as designed is not the same thing as a real system**. A system as designed typically consists of engineered components, operators (who are assumed to behave as predicted), and planned maintenance activities, plus the safety critical components have substantial supporting evidence. The real system also has the physical parts (which may change over time), the human operators (who adapt, react, and become habituated to their work), and human maintainers (who adapt, react, and can get inventive in how to keep a degraded system operating). The real system may also include myriad interconnected human/technical/financial systems which can: fund or de-fund; investigate or fail to investigate; govern or fail to govern; facilitate or disrupt operations. Each system agent has priorities and incentives which may align with or may be in tension with each other. The real system is the one that experiences real-world trigger events or stressors, and thus resilience engineering focuses on the real system, because "understanding the functioning of a socio-technical system is the necessary and sufficient basis for understanding how it fails." [1].

2) **As modern cities get larger and society becomes more technologically advanced, our systems become more tightly coupled and interdependent, making us more vulnerable to multi-system shocks and stressors and making resilience more important**. More than ever before in history, our systems are interlinked at scale and across categories [7]. An event can cause cascading and unforeseen knock-on effects in other systems and the impacts can be felt across a large population: especially for systems of government, finance, defence, critical infrastructure and communications.

1.1.1 Australian resilience legislation

Australian federal and state governments have put in place policy and legislation targeted at improving the resilience of our cities. The Federal critical infrastructure policy explains the need for a common, legislated approach: "…Extreme events and stresses, including those that may be unprecedented but are no longer surprising, have disproportionate effects on critical infrastructures and hence on communities, cities, and megaregions."[8] In the legislation, rail networks and communications networks are categorised as a critical infrastructure.

The legislative framework formalises monitoring of organisational interfaces and mandates cycles of improvement at multiple scales to strengthen each city's response to stress and crises. The foundation is information sharing partnerships between Government agencies, infrastructure owners / operators and corporate agents. These organisations must also be active in improving resilience: coordinating a response to a crisis scenario (desktop and real-world exercises), followed by constructive critique and continuous improvement.

1.2 Two different philosophical views of the same physical world

Resilience engineering departs from most other engineering disciplines in that it uses complex systems thinking, rather than the command and control (complicated problem-solving) philosophy of most other engineering disciplines (framed by Dekker in [3] as authoritarian high modernist thinking). The real world is unchanged – the key difference is in how we make sense of it, seek to control it or work within it and in how we frame actions and understand outcomes.

A complicated problem-solving framework is useful where one person can understand, model and validate the workings of the entire system – such as the interlocking logic of a large junction. A complex system can't be understood in its totality by one person, nor can it be usefully simplified. Complicated problem-solving thinking yields problematic forecasts and erroneous conclusions. Table 1 illustrates the key difference between a complicated problem-solving mindset and complexity thinking.

Table 1: The world from a command and control perspective, in contrast to the view from complexity.

Command and control thinking (Complicated problem-solving)	**Complexity thinking (Complex adaptive systems & resilience engineering)**
From: [3] p. 134	
A central controller manages the system from a centre at the top.	There is no centre, or top. Through relationships and interactions, parts of the complex system self-organise, horizontally. This can give rise to new behaviours (emergence).
Everything can be controlled.	Almost nothing can be controlled in a complex system. But because they reverberate through webs of relationships, actions somewhere in the system can influence almost everything anywhere else.
A central controller can synoptically understand and direct the whole system.	Nobody can understand a whole complex system, because then that part would have to be as complex as the system (which then means the system wouldn't be complex). Each part in the system only has localized knowledge afforded by its particular perspective.
The more standardised a system and its components and the more standardised their functioning, the better it works.	The more diversity there is in a complex system, the more resilient it is: able to withstand and absorb unforeseen disruptions and challenges and create new behaviours in response.
To understand something, the controller needs to go down-and-in, take things apart and look at individual components.	To understand something, we need to go up-and-out and look at interactions and relationships.
If the system doesn't work, the controller can trace it back to a broken, non-compliant or deficient component (which in turn can point to inadequate control).	It is not easy to say whether a system works or not (it's not binary in complexity), but its functioning emerges from interactions, not from individual parts.
The behaviour of the system is a direct, linear and proportional result of how its components are controlled. Cause and effect are proportional.	The behaviour of the whole system emerges from an ever-evolving complex web of interactions and relationships. Small changes can lead to enormous effects. And enormous disruptions can be dampened to almost nothing.
A system can be stable, operating as predicted.	Systems have points of equilibrium and what seems like stability but this is understood as dynamic equilibrium, where the system is temporarily held steady between powerful forces and objectives pulling in different directions.
From: [11] pp. 34, 63, 88-91	
Only directly connected components communicate or affect each other. An example is given of cogs and gears in a mechanical system.	System elements are interdependent: Feedback and communication between system elements is key to understanding the system state. Positive feedback amplifies a variable; negative feedback mediates the variable. Delay, gaps in communication and secondary feedback mechanisms have a large impact on the system behaviour.
Damaged components can be repaired and the system will recover to work as before.	Systems adapt to absorb shocks up to a threshold or breakpoint: beyond which change can happen fast and/or can be difficult to reverse or stabilise.
The controller's attention should be focused wholly on the component of interest.	A system cannot be understood or successfully managed by focusing on only one scale. The effectiveness of interventions and the flows of resources and information across systems at one scale depends heavily on larger-scale (bigger and much slower) and smaller scale (apparently insignificant or apparently instantaneous) system dynamics.

2 RAIL AS A SAFE SYSTEM

Rail has a strong history and core philosophy of safety based on conservatism and compliance. Hale and Heijer (Chapter 9 in [1]) propose that (European) railways take "an extreme version of a command and control strategy". Many Australian rail engineers would be very comfortable with their description of rail safety:

> *"Passenger safety appears to be achieved by defining very clearly in advance what are the necessary prerequisites of safe operation and forbidding operation outside them. When the system moves outside this clearly defined safe envelope, the railway system stops, regroups and restarts only when the necessary operating conditions have been re-established."*

Signalling systems in particular have been treated as complicated problems rather than complex systems. Behaviour is kept within modelled limits and comprehensively tested before 'going live'. Predictable behaviour is the goal of our network rules. Fail-safe and redundant design is core. Governance focuses internally, on safety

assurance of both content (inner workings of the system) and process (competence, stage gates, independence of reviewers and testers).

Modern railway (and signalling) systems and rules have adapted to an accumulation of historical catastrophes - and compliance to those rules and procedures is the foundation of what we believe to be safe railway operations. Safety in design looks backwards to prevent all historical accidents, rather than looking sideways to other industries or looking forwards to pre-empt emerging risks. Woodbridge [12] observes that "signalling has evolved by accident": i.e. accidents are the primary driver of technological advances and rule changes. He proposes that different railway networks have different signalling principles because high-consequence accidents trigger a rule change locally and lessons from minor accidents or lucky escapes become "quickly forgotten or ignored". For example, "the implementation of AWS and TPWS followed pairs of [serious] accidents in quick succession." ([12], pp 322)

Almaberti ([6], also chapter 16 in [1]) proposes that high-risk complex systems such as rail (transportation in general) are "ultra safe systems"; where a serious accident or adverse event may trigger a crisis of public confidence for all operators. In this category of system, there is often a high level of supervision, control, legislation and progressive increase of standardisation and reduction of freedom to adapt within these industries. Almaberti (chapter 16 in [1]) and Dekker [3] both propose that ultra-safe industries have gone beyond the "sweet spot" of just the right amount of procedural compliance, into the next region where compliance has no marginal improvement on safety or potentially into "overcompliance" where actual risk is increased.

In recent decades, rail has been challenged by the speed and low cost of technological change, greater connectivity with external systems and leaps of technology e.g. in sensors, computing, predictive algorithms, artificial intelligence and other areas. Adoption of new technology seems more cumbersome in rail than in many other industries: perhaps this is due to the procedural burden of an ultra-safe system, perhaps due to the need to maintain engineering protections against all historical accidents, or perhaps due to the way the command and control way of thinking shapes our approach to change.

2.1.1 Conventional safety: complicated problem-solving

Safety, under the complicated problem framework is achieved by first minimising or engineering out things that can go wrong from a position of high-level authority, then requiring rote obedience to those systems and processes. Examples include:

- Conventional workplace safety (Safety I, in [2]). The philosophy is of central regulation: In Australia, Worksafe legislation underpins the rules and specifies minimum worksite and workplace procedures to manage safety.
- Conventional systems assurance of safety-critical systems in rail. The philosophy is to engineer dangerous failure out: assuring safety by including sufficient planning, process controls, inspections, tests and integration activities etc. to give confidence that unsafe failure modes are statistically near-impossible.

2.1.2 Complex safety and resilience

Safety, from a complex systems perspective, is highly contextual. Application of apparently simple rules in different contexts can produce widely varying behaviours which are not easily predictable. The complex system safety perspective (Safety II, in [2]) perspective illustrates that the target of 'zero harm' safety is also not meaningful in a complex system:

- The 'iceberg' theory of safety is flawed. The correlation between small hazards and incidents and big hazards incidents is either non-existent or negative: excessive focus on identifying and preventing small accidents is a repeated feature in organisations which have allowed practices to degrade to the point of major catastrophe (such as Deepwater Horizon) [6].
- Practice (at crisis management) makes perfect. Small and regular safety incidents may be useful: they maintain the capability of the system to swap to 'emergency mode' and control or counteract potential cascades into catastrophe. The case study in section 4.3.1 illustrates the benefit of this practice.
- Safety decay is not linear. Performance can be stretched up to a limit (a safety-performance boundary [1]) with no meaningful increase in incidents. Close to the limit, warning markers may appear: the system may

be able to adapt and compensate. Beyond the safety-performance threshold, the cascade into crisis has a high probability. It may happen slowly or quickly, be a graceful degradation or an abrupt collapse and recovery or adaptation may or may not be possible. [1]

2.1.3 Case study: Train control of the Melbourne City Loop

The Melbourne passenger railway network provides a case study of managing a complex system near the safety-performance boundary. The system layout has a notable feature: all radial lines come into a 4-track bi-directional City Loop, with two at grade stations and three underground stations. The City Loop allows passengers commuting into the city the convenience of remaining on the train as it circles around the central business district (CBD). The radial rail network architecture services the economic and high-rise development on the CBD..

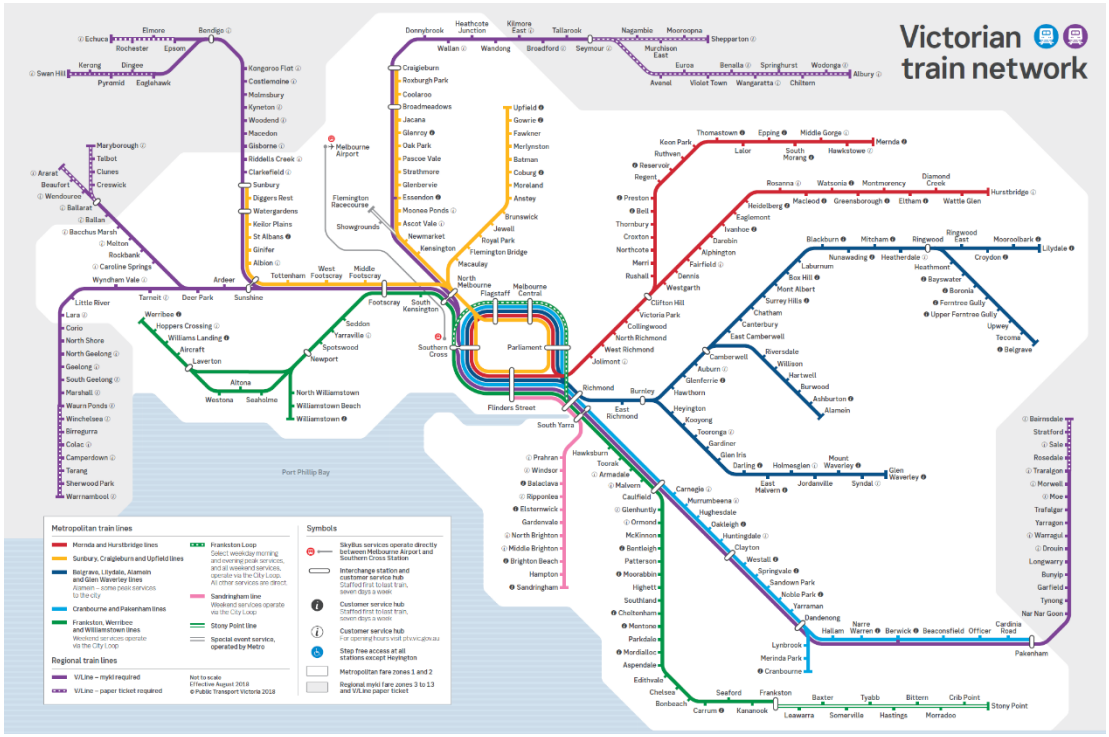

Figure 1: Melbourne rail network map, with the City Loop at the centre. Source: [9]

The City Loop is signalled for 30 trains per hour on each of 4 underground lines. At peak time it often runs at peak operational capacity of 24 trains per hour. It is understood to be a rail network bottleneck – the limit on trains per hour has not changed since 1985 when the loop was commissioned.

The City Loop is also understood to be operating close to the safety-performance threshold. Passenger demand has increased year-on-year, to the point where – despite re-fitting trains twice to have greater passenger capacity, some lines still experience substantial passenger crowding during peak periods. In this context, there is very little 'slack' in the performance to absorb or buffer a trigger event. Due to the city's reliance on rail commuting, a trigger event that disrupts train services during the peak puts passengers at risk of crush or crowd-related injuries. Disruption is further explored in the case studies in Section 4.3.1.

To manage the City Loop, a specific control desk is tasked with the fluid reallocation of train identification numbers at Flinders Street (where the train services officially terminate) to absorb minor delays and manage and recover from major trigger events. There are no stabling facilities at Flinders Street, so stopping rollingstock at this station at peak hour can in itself be a trigger event for a substantial network disruption, with knock-on effects for some hours. Over years, the control centre has adapted and evolved its practices to manage disruptions from the outside world: for example, there is a permanent liaison desk to interface to police and emergency services and assist coordination of events.

3 RAIL AS A SYSTEM IN CONTROL - OR AN ADAPTIVE SYSTEM?

3.1 A command and control perspective on rail

Conventional perspectives on rail project management would seek to provide the following (from [3], p 37):

Standards: Structured expectations - and capability to measure against those expectations. In Australian rail, as with rail worldwide, the ideal would be to have a fully documented set of controls around:

- What work is done (a hierarchical structure of written standards explaining the minimum performance or prescriptive requirements plus deemed to comply solutions for a particular context)
- How work is done (process control and resource allocation throughout the asset lifecycle)
- And by whom (a full competency management system and safety assurance of tools/automation).

Central control: A single central point of accountability within a single organisation who is tasked with achieving the expectations and who has (and can delegate) authority to compel people to behave towards these targets. Ideally, this 'one railway' approach would place a Railway Commissioner (or similar) with overall accountability.

Synoptic legibility: The system is planned, understood and simplified to the point where the single central point of accountability can monitor the whole system against its expectations, spot non-conformance and intervene. Behaviour is tractable, modelable and kept within those modeled limits.

3.1.1 Standards and legislative governance in Australia

Rail across all of Australia has never had a robust top-down central standards control body and does not yet have a coherent national standards framework. The Rail Industry Safety and Standards Board (RISSB) has begun the task to backfill one, mirroring successful similar endeavours in the UK, EU and elsewhere. Such fundamental definitions as track gauge, signalling principles, safeworking practices and type approved technology vary across networks and state boundaries for historical rather than operational reasons. Networks have struggled to align standards across all levels. This is understood to cost hundreds of millions of dollars a year to Australian rail projects and operations [10]. Even where the fundamental operational parameters can be agreed, control and accountability may not be clear: at a single location, multiple standards authorities may have jurisdiction. The track and wayside infrastructure may be a mix of private and State owned, with multiple lease or franchise agreements for different assets. Third-party entities may be engaged for maintenance and renewal. Different project structures add to the confusion: a scope of works may be managed by one or more public, private or public-private-partnerships. The questions of – who is responsible for getting the standards right? And who imposes what sanctions on which organisation in case of non-compliance? – are not simple to answer. The contrast to the mature standards hierarchy enjoyed by the European Union is shown in Figure 2.

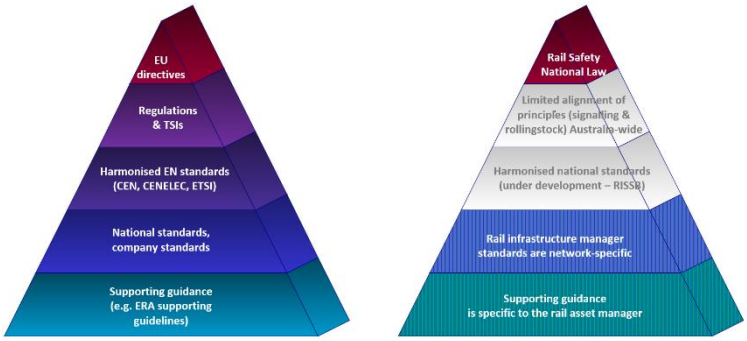

Figure 2: Mature EU standards hierarchy in comparison to the developing Australian standards context

Standards serve the important purpose of providing concrete parameters and clear guidance to designers, bringing certainty and structure to ambiguous or messy problem spaces. Good standards can make a complex problem merely complicated: without them, project design solutions are not repeatable and conventional project management will struggle.

The current state in Victoria is that every project requires stakeholders to separately negotiate and agree on these fundamentals: responsibilities and accountabilities for project delivery, workplace safety and system safety; what work is done (scope, budget and standards baseline); how it is done (process governance, gates and milestones); who can do the work (accredited competency – the national framework has multiple interpretations) and the authority and approval process for each element. Consternation reappears many times over the technical solution for both signalling and rollingstock – especially for the balance between established type-approved technology and project-specific innovations; over the fringe interface definition for connection to existing infrastructure and integration responsibility; and over information ownership: intellectual property, liability and asset information.

The contractual relationships between the asset owner, the operator, the project lead contractor and subcontractors are often as or more important in deciding the outcome of these negotiations and the shape of the physical assets, than the engineering solution.

3.1.2 Central Control

The extent of central control varies markedly between different rail networks across Australia. The mining railways, including the Rio Tinto and BHP iron ore networks in the Pilbara, have strong central control and vertical integration. This allows a clear link to be made between top-down strategy and decisions made at all levels in projects, maintenance and asset management and provides a common point of escalation of issues across rollingstock, signalling, track and civil and ports.

The contrast is Victoria's urban and regional rail network, where central control is very limited.

The Victorian government has strong oversight in both the project space and operations/asset management space – but changes within government departments have sometimes had these organisations reporting to different ministers. The democratic cycles and economic trends of the last 50 years have led to cycles of expansion and contraction of the transport governance function, causing flux in the staffing levels in these departments and varying enthusiasm for active intervention in the railway. In the 1990s, the government at the time pushed for privatisation of rail and market leadership, which resulted in the break-up of the network into different areas and asset types and a period of fragmentation and technology stagnation. The current government has sponsored a major program of works to update and renew the urban network. Section 3.2.1 explores repeated investment booms in the context of a 150-year pattern of boom-bust cycles.

3.1.3 Synoptic legibility

Synoptic legibility is the ability of a controller to understand and observe system behaviour and intervene if necessary. The task of signalling is to improve synoptic legibility for the railway. The task has not changed since 1833 although no longer done by men at station houses every mile (extract from "Railway Companion", in [12]):

> *"The [Liverpool and Manchester Railway Line] Company keep a police establishment who have station houses at intervals of about a mile along the road… The duties assigned to these men are to guard the road, to prevent or give notice of any obstruction, and to render assistance in the case of any accident occurring; and to do this effectively they keep up a continual line of communication."*

Other types of synoptic legibility may also be sought from the signalling system or related systems:

- Position, speed and fault status of trains; fault status of infrastructure
- Passenger status and location: ticketing, security, special needs, medical incidents etc.
- Logistics management for goods or bulk material
- Asset condition, including monitoring for change or decay and controlling maintenance activity
- Project activity: status and planned impact
- Interfaces with other types of transport for goods or passengers

Signalling synoptic legibility can be assured by providing a signalling system that covers the rail network to the appropriate granularity for that network's task and risk profile. This is why there is no 'one size fits all' signalling

system: the needs of Australia's long and stringy interstate network (8500 km of track, 450 trains per day) are very different from Sydney Trains (815km of track, 2708 trains per day [17].

The command and control philosophy (to suit complicated problem-solving) would endorse signalling's approach of adding systems to close the gaps in synoptic legibility. Peter Woodbridge [12, pp. 322] summarises:

> *"The lessons learned from accidents have been used to improve signalling so that there are more effective barriers in place between the existence of a hazard and the occurrence of an accident:*
>
> - *Initially the focus was primarily on adding technology to guard against mistakes by signalmen;*
> - *Then more attention was given to adding technology to guard against mistakes by drivers;*
> - *With the increasing automation of these functions which in normal operating conditions largely often eliminates the human from direct control, this intensifies the dependence on the increasingly complex technology;*
> - *Concentration now needs to be on reducing the chances of human error during the specifying, development, application design, installation, verification and validation, operations, maintenance, upgrading, renewal and disposal phases of such systems; otherwise errors in these systems could be the direct cause of an accident. Automation of these processes should help; however this just moves again the opportunity to get things wrong to the people who design that automation."*

Woodbridge then rather beautifully puts his finger on the flaw in the last step of authoritarian logic:

> *"In the past if a person made an error then in general an accident would either result quite quickly or not occur at all; nowadays it is a more indirect involvement. There is typically a rather longer time period between cause and effect and each person only makes a contribution to the totality of what went wrong; this makes it both harder, and also more important, to learn what we can from accidents and incidents."*

In other words, complexity (interactions, interfaces and delay) in the signalling system reduces the overall synoptic legibility of the railway further with each extra layer of engineering problem-solving to the point where we can no longer trust it. Signalling technology has just reached the point where it is more usefully thought of as complex, rather than complicated.

3.2 The complex system adaptive cycle perspective on railways – Australian and overseas

Complex systems principles offer a way to understand and alter system behaviour. The boom-bust cycles in Australian rail history more closely resemble an adaptive cycle out of ecology ([11], p.83) than a planned hierarchical structure.

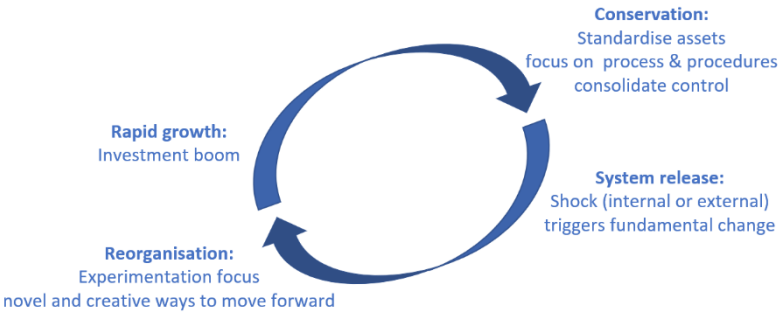

Figure 3: A simple representation of the Adaptive Cycle [11] tailored to rail and other infrastructure

3.2.1 Railways in rapid growth phase

Australia has had multiple boom-bust cycles in rail, with these events marking the rapid growth phase of investment booms:

- The Gold Rush boom in the 19th century expanded the state railways of the Australian east coast and left extensive rail land assets with these States. In Victoria, this land still remains State-owned land.
- The 20th century had several boom-bust cycles. The "roaring" 1920's electrified the radial suburban network for Melbourne. Subsequent cycles of expansion and contraction responded to both the economic climate and the wider trend of changing preferences for transport modes. The legacy is solid and enduring transport infrastructure – even if the City Loop now poses challenges for high-capacity metro (Sections 2.1.3; 4.3.1). The freight rail networks that developed in these boom times have been partly brought into a national freight network run by the Australian Rail Track Corporation (ARTC) under federal governance [13].
- The mining boom of 2004-2016 focused on the iron ore and coking coal export chain especially in Western Australia, New South Wales and Queensland. Today, the mining companies that build their own infrastructure have the most robust central control [17] (also see Section 3.1.2).
- The current rail investment boom is the largest (in real value) since the 1880's Gold Rush, with over AUD$100b allocated or spent in Victoria alone [21]. Projects cover suburban, metro and regional passenger rail, intercity freight rail and intercity high-speed rail. This boom was triggered by wider forces, including global low interest rates, rapid urban population growth, the 4th industrial revolution and the positive public (and political) percception of rail as a clean, safe, low carbon transport mode of the future. These megatrends are elaborated in Section 3.2.4.

3.2.2 Railways in conservation phase

At the end of a rapid growth phase, the conservation phase typically marks a shift to longer-lived, more conservative organisations which are more efficient in their use of resources [11]. Organisations merge and slow their growth, seeking economies of scale and accumulating capital reserves. Processes are strengthened, regulation is tightened, standardised technology and cautious leadership seek to bring the unruly infrastructure "under control". As an illustration of this transition, the standard station building shown on the left of Figure 4 below was created in 1888, towards the end of the post Gold Rush rail boom [13] – and this initiative is rather eerily echoed in this investment boom, where the initial rapid growth phase of the Victorian Big Build has rediscovered the cost-effectiveness of standard station design – at roughly the halfway point of investment. Bespoke responses to every site incur design cost and assurance burden. Repeatable, controlled, efficient solutions are favoured.

Figure 4: A plan for standard station buildings from 1888, in the consolidation phase of the Octopus Act rail boom; and a station design proposed for design re-use in 2018, in the consolidation phase of the Victorian Big Build.

The late conservation phase is worth bringing to attention: the investments made in each growth phase 'boom time' lock in system choices which must then be made to continue to work safely in the investment lull. The rail networks do not remain static: physical assets degrade and must be repaired; practices in the human system evolve and adapt. This phase is typically a period of resource constraint, resulting in chronic stress and repeated crises. Rail may not be a focus of investment. Governments and private organisations may seek to reduce workforces, move funding elsewhere. The system may be stretched closer to the performance-safety threshold, with repair and renewals postponed. Carefully curated information and lived knowledge may be lost in this phase.

3.2.3 Railways in release phase

The release phase is described in [11] as "a disturbance that exceeds the system's resilience and breaks apart the web of reinforcing interactions".

From a single signalling system perspective, it would be fair to say that each incident or accident triggers a release phase when it highlights the behaviours or activity that exceeded the system's safety measures as they were designed. This is at a smaller scale than the scale of interest here: Section 4.2 discusses interactions between systems at multiple scales.

From a whole of railway perspective, a release phase has been a sequence of events that highlights that the current ways of working are not actually working. These are relatively rare.

An example of catastrophic system release is outlined in the Woodbridge chronology of UK railway signalling [12]. The UK had a sequence of extremely serious rail accidents from 1988 to 1991: Clapham Junction, Purley, Huddersfield, Reading, Stafford, Severn Tunnel and others. Common themes across multiple accidents of signals passed at danger, decayed maintenance and safety processes, failures of supervision, failures of training, degraded and unreliable physical assets, and failure to manage degraded situations ranging from the apparently benign (e.g. hand signalling at Huddersfield) to the extremely serious (e.g. management of the evacuation at Severn Tunnel).

In hindsight, this period is recognisable as a release phase because it triggered a major reorganisation of legislation, and also contributed to the privatisation of British Rail and the ultimate failure of Railtrack (although it can be argued that the privatisation was also politically driven from external processes). In the reorganisation phase that followed, the IRSE emerged to curate signalling knowledge, champion industry training and competency; drive trials and plan the rollout of many new technologies. This has led to significant measurable improvements in safety and restored public confidence in rail.

Another example of system release is China Railway. [19]. In 2004, there was a decision to re-organise the national rail system into three levels: urban mass transit with low speed and high density, inter-city rail with medium speed and high density, and high speed railway for long distance transportation. In hindsight, this can be seen as the point of system release: the previous system's capacity to service the transport needs of China had been exceeded, and recognition of this in high-level government strategies, combined with accelerated economic growth aligned with increasing population and urbanisation, became the trigger for major system change. The reorganisation has allowed China high speed rail technology to become the world leader in scale, precision and low cost: rail transportation network planning expects the total length to exceed 30,000 kilometers in 2019[18].

3.2.4 Railways in reorganisation phase

The reorganisation phase immediately follows a system release, when all options are open. This is the phase where novelty can thrive: small players can appear and seize control or change the direction of the system [11]. The early 21st century is seen as a reorganisation phase at a macro scale, covering the whole planet and all of humanity. Moises Naim [7] describes this reorganisation phase as springing up from the dispersal and decay of the centuries-old machinery of power. He proposes that it consists of three concurrent revolutions:

- A 'More' revolution: an age of profusion of wealth, comfort, quality of life, luxury and longevity;
- A 'Mobility' revolution: unprecedented immigration and urbanisation, instant communication, expectation of safe and efficient transport – and mobility of identity in the form of unprecedented opportunities for travel, education, ability to alter class and status and rapid redistribution of wealth;
- A 'Mentality' revolution: a deep change in expectations and standards where a population rapidly assumes that standards, resources and technology that were previously unachievable or exclusive luxuries are now theirs by right.

The impact of this macro reorganisation on rail in general – and Australian rail as the focus of this paper – is not yet clear. This is a source of some unease in our industry. The speed of change of digital technology outside rail has been met with distrust. According to conventional safety assurance frameworks (described in 2.1.1), untested technology is by default forbidden for safety critical systems and must be assured safe in isolation, then in context. This is a key barrier to rapid innovation and adopting solutions from other industries. There is a jarring contradiction between the faith in conventional safety processes and observations from outside rail that the (non-safety-critical) tracking of a pizza to your door is cheaper, easier, plus potentially more reliable than signalling train detection technology from only a few decades ago.

In Victoria, there has not been a major release and reorganisation in the rail industry. Even in the current construction boom, a greenfields project is never truly 'greenfields': the land purchase and some infrastructure may date from the 1880's, the track alignment and station location from the 1960's, the signalling architecture and interfaces must be made to work with 2000's-era technology in the control centre and fringes. Specifying a project in a network with this kind of history is a complex task: the project must contend with a patchwork of technology which has evolved and adapted: not the clean system specification we would hope to see in a project.

Sydney Metro has taken a different approach. The project structure for the Metro Northwest line seeks to make the new line a clean break from legacy systems. The scope of the City Stations work package is "a brownfields project to enable a greenfields project": to detach the central stations and key legacy interface points of the new line from existing rail lines [20]. Compartmentalisation of rail systems – deliberately reducing the interdependence and interconnectedness of lines, networks, control territories and jurisdictions – is one way of realising the opportunities from a reorganisation phase of the complex system adaptive cycle. Crafting the interfaces between assets to match the organisational accountability is a useful technique to reduce the engineering problem to merely complicated in

a complex organisational environment. This and other techniques to manage complex systems will be explored below.

4 PRACTICAL GUIDANCE ON RESILIENCE ENGINEERING

Resilience engineering proposes a general set of principles that can be adapted to human-technical systems, or to a macro system such as a city or a national rail network, or a smaller system such as a single engineering department in a single rail operator and the safe operation of the equipment for which that team is responsible.

A set of common traits or characteristics of resilient systems have emerged from the literature. These principles appear to hold across disciplines and scales of activity. These include [1]:

- Buffering capacity to absorb disruptions;
- Flexibility versus stiffness appropriate to context;
- Monitoring of margin to the performance/safety boundary;
- Tolerance at the boundary, i.e. graceful degradation vs rapid collapse;
- Cross scale interactions:
    - Downward, how high level structures create or resolve pressures and contradictions,
    - Upward, how local changes influence strategic goals.

4.1 Focus on boundaries, interfaces and interactions

A resilience engineer cultivates a preoccupation with system boundaries, because the interfaces and interactions between system components are important for understanding or adjusting system behaviour [1].

Good use of boundaries can reduce a complex problem space to the merely complicated and improve the effectiveness of conventional engineering problem-solving. The resilience engineer should focus their attention on feedback at the boundaries of system components. Feedback between system levels is one of the first features to decay. Command and control thinkers may not see this as a problem, because in that paradigm each failure is contained in one system. Some tips for resilient management of system boundaries are:

1. System safety assurance should generally include both:

    - Component-level assurance of the system as designed (as in section 2.1.1) and
    - Assurance that there is effective communication across interfaces in the real-world system (as in Section 2.1.2, also [1, 2, 3, 4, 5, 6, 8]).

    The return on effort/cost for formal (complicated) safety assurance in the adaptive (complex) real-world environment may be questionable [3, 6].

2. Feedback must be fast and accurate. Resilient behaviour in the face of a crisis or shock requires elements at multiple scales to know quickly that there is a crisis or shock. Hollnagel et all [1] include multiple case studies across industries where the decay or absence of feedback enabled a shock to become a cascading catastrophe. Woodbridge [12] provides multiple examples from the UK where a catastrophe could have been prevented or mitigated with timely human-oriented feedback or better understanding of the limits of technical system. Abbots-Ripton (1889) could have been mitigated by more effective communication, signaller-to-signaller or driver-to-guard. Quintinshill (1915) could have been prevented or mitigated by more effective system monitoring of the location of the troop train, by signallers, firemen and drivers. Severn Tunnel (1991) could have been mitigated by effective radio communications or understanding of the reliability limits of the telemetry.
3. Organisational boundaries should ideally match the technical edges of the system: this gives the best chance of conventional problem-solving being effective. For example, regarding Severn Tunnel, Woodbridge describes the mismatch between integrated technology and fragmented human teams: “Although the department of British Rail was named “S&T” [Signalling AND Telecoms], it actually operated as two almost separate organisations, so there was an interface issue resulting in the use of pairs of a Telelcoms cable for a signalling asset.” ([12], p. 401).

4. Feedback is a great way to test and assure new technology. Experiments can be run using shadow mode (with new technology installed on an area already covered by existing technology to validate that the systems behave the same way), A/B tests (where two systems are set up differently to compare performance) and trial on 'test lines', (where an experiment has low consequences). Feedback should be fast and accurate, particularly focusing on aligning the technology and the human system and on looking for opportunities about human-led improvements to the system-as-designed.
5. Modular architectures are very useful. With standard interfaces, each module can be treated as a 'black box'. The ease of modern communications which underpins Naim's "mobility revolution" is based on 'black box' principles, where interfaces are standardised, and components are fully interoperable and backwards compatible. In rail, there is some work to do on international standards (e.g. ETCS) to achieve full modularity and interoperability.
6. Feedback can trigger change across a boundary. If a problem is identified in a system but the organisation/scale of interest is resistant to change (perhaps showing rigid control behaviours in the late conservation phase), pressure and feedback from across an interface can be more effective than persisting with unheeded warnings internally.

4.2 Understand the adaptive cycle at multiple scales

Resilience engineering offers tools for visually mapping the cross-scale interactions in a complex system context [11]. Figure 5 shows this applied to the Victorian Big Build, including the wider macro reorganisation described by Naim in [7] (the Fourth Industrial Revolution), and the smaller adaptive cycles and lifecycles of design packages and projects. Each of these subsystems is navigating an adaptive cycle, with an estimate of the cycle length shown in log scale on the x-axis.

Understanding of timing is critical. Changes involving innovation, major organisational or technological realignment and experimentation are most effective in a reorganisation or rapid growth phase. Moving towards standard and repeatable solutions is most easily done in an early conservation phase. Shifting entrenched non-compliance is most effective with a powerful agent and a late conservation phase. And when a release phase is triggered, intervention must be swift, both to prevent destruction and put in place the building blocks of the next cycle.

When mapped out at multiple scales, the organisations in the Victorian Big Build and the government asset planning functions are at all different stages of the adaptive cycle. The different timescales of each adaptive cycle can be frustrating, but each system moves at its own pace and with a systemic mindset this can be navigated. Figure 5 illustrates.

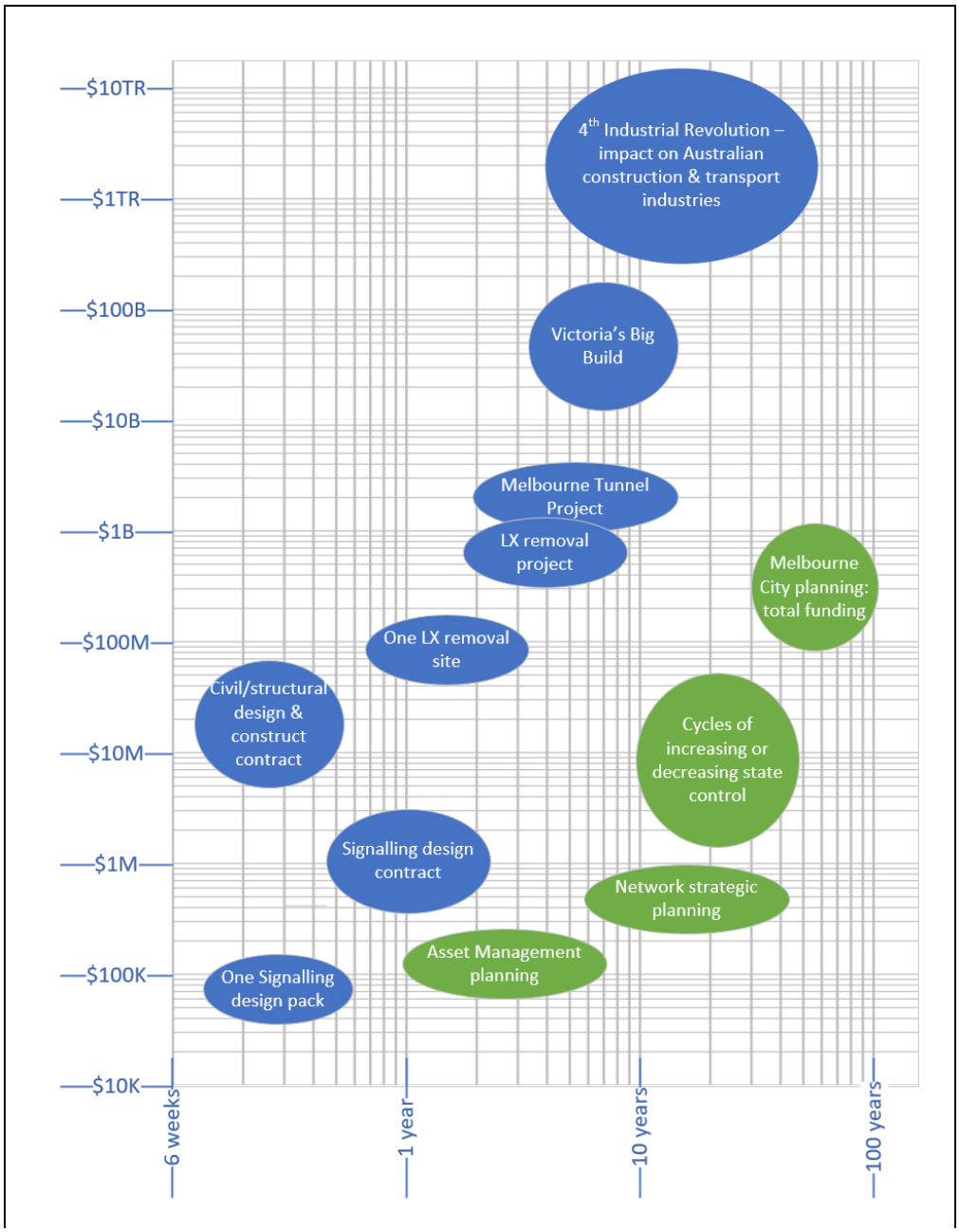

Figure 5: Adaptive cycles relevant to the Victorian Big Build, using logarithmic financial value and time scales

4.2.1 Case study: Systemic change to enable 3D signal sighting processes

In 2016, the Level Crossing Removal Project had packages where civil construction progressed without ensuring that signal sighting was complete, resulting in late rework at multiple sites and suboptimal signal positions. 3D signal sighting was put forward as an innovative solution, using the same graphics engine used for civil design planning and assurance. [22] In practice, getting this trialled and formalised required of use multiple adaptive cycles:

- By the time the first issue was identified, the site was nearing completion and entering the release phase (demobilisation). This is not a good point to run an experiment or create a new process.
- The two contractors struggled to collaborate or innovate across timelines. A signalling design pack is slower (longer timescale) and less powerful (lower spend) than a civil/structural design pack. The civil construction contractor did not want the build schedule compromised – so determined that neither the package underway, nor the next package, would be appropriate for innovation.

- One level higher, the Level Crossing Removal Project and the Melbourne Tunnel Project both saw clear value in solving the repeated signal sighting problems – but their mindset was heading into the conservation phase. The 3D signal sighting innovation was not prioritised.
- The fuel for the 3D signal sighting trial finally came from individuals who had the rapid growth mindset of the 4th industrial revolution and were willing to run a potentially disruptive experiment using 3D models, virtual reality headsets, and collaborative processes. It was first run as an A/B test alongside conventional signal sighting. The technique was highly effective in de-risking the civil/structural contract. The individuals were quickly able to scale it and have it adopted by an upcoming Level Crossings site.
- The Level Crossing Removal Project was then able to draw on the strong control focus of their own conservation phase to lock in (structure and formalise) the new 3D signal sighting technique. This took some months, consistent with the slower timescale of this organisation. The process is now open to other worksites.

4.3 Use cycles of disruption as opportunities to actively improve

One of the major tools of resilience engineering is actively learning from real crises and rehearsed crises. The Australian resilience legislation in Section 1.1.1 focuses heavily on the formal rehearsal of crises – both desktop and live. But the best predictor of a system's response to stress or crisis is its actual performance under stress and crisis. The following case study contrasts a command and control response (focusing down-and-in to component parts) response with a complex systems response (focusing on interface and the broader perspective) – and nicely illustrates the key points of Hollnagel, Leveson, Dekker, Almaberti and others [1, 2, 3, 5, 6] that the mindset of actors during a crisis – whether the problem is understood to be complicated or complex – has a major impact on how it cascades or is buffered.

4.3.1 Case study: similar major network shutdowns with contrasting responses

Network shock and conventional command-and-control response: "Trainageddon", July 13, 2017:

At approximately 4PM, the Melbourne train control system experienced a malfunction and stopped all train movements on the city's radial network in the afternoon peak. 224 services were cancelled and 337 services ran late. Station platforms, forecourts and surrounding areas were crush loaded with commuters seeking to get home. Trams, buses, taxis and Ubers were unable to manage the crowds, with Uber surcharges running at 3.6x. Upwards of 175,000 people were affected. [14]

This was the first network-wide disruption for some years, and there had been no opportunity to deliberately rehearse such a crisis. Focus during this shutdown was down-and-in: on the technical issue of fixing the computer glitch, rebooting the control system and connected systems, then restarting trains. Train services were re-established after 5:45, nearly two hours after the failure.

Social and news media were highly critical of passenger treatment, citing inconsistent passenger information, safety risks and minor injuries from crowding and crush points, and lack of coordination with other services and transport modes. The train operator refunded travel cost to commuters and was also required to pay a fine of AUD$1.2M for non-performance. [15, 16]

Network stress and a resilient system response: planned shutdowns of the City Loop, Jan 2018, Jan 2019 and April 2019

In January 2018, the Level Crossing Removal Project works required the rail operator to shut down the City Loop for 8 days. This was the first long shutdown of the City Loop in over 30 years. The disruption planners were struggling to see how they could move the 300,000 passenger trips per day, but drew on lessons learned from "Trainageddon" and international best practice in transport resilience.. The high-level approach taken was to time the shutdown for January, as this is typically a period of lower patronage (25% reduction on demand), to use buses as train replacement and to run a public information campaign to encourage travellers to plan ahead, stay home, reschedule travel outside the peak, or mode shift to other types of transport. The shutdown focused on the inner city area: outer rail lines remained operational up to a passenger interchange point ~10km from the CBD.

On the first day of the peak, the rail operator's approach was to simply "put buses out there". Over 200 buses were deployed each day, but this was still well below the rail system capacity. Passengers experienced delays upwards of 3 hours in the peak. Over the next 7 days, techniques from city resilience and emergency management came into play: cross-organisation information sharing was a priority, with twice-daily meetings between the rail operator, the roads authority, the project and the City of Melbourne council to discuss what was working and where problems had arisen. Customer service staff were flexibly allocated to pinch points to guide passengers and inform them of progress. Status updates were broadcast via news media. Passengers became seen as part of the solution – they were able to spread information and make decisions that eased the congestion with each shift. By the end of the shutdown, passenger delays had been reduced to less than 1 hour.

In January 2019, planning for the second 8-day shutdown had incorporated lessons learned. End to end bus route analysis had identified opportunities for improved road traffic control, such as live adjustment of the traffic light cycles to prioritise buses. A dedicated disruption control centre was set up alongside the train control centre. CCTV was installed onto the road network to remotely monitor congestion at pinch points and mode transition points to monitor passenger safety. Communications were increased: a combination of TV, radio, social media, print, billboard, handout and direct community engagement drove a reduction in peak demand. A target of 20% mode shift of patronage was set, but 30% mode shift achieved. Some commuters reported only ½ hour delays.

April 2019 was the most challenging shutdown. It was the longest duration (35 days of partial or complete rail shutdowns). A communications saturation campaign achieved 45% mode shift, again exceeding the 40% target. Disruption control included autonomous sub-teams with separate tasks, reporting methods and technology. The bus supervisor network reported to the "bus control desk", using train control techniques. Customer service included a team of passenger counters, using tablets to gather data and predict pinch-points before they arose. All staff had radios. The different GPS locator systems from each bus company were integrated with disruption control to provide realtime transit time data to passengers. Passenger comfort was also a focus, with shelters at all waiting points and buses offering a choice of CBD destinations. Each shift ended with a team leader discussion about opportunities to improve the passenger experience. Initially, delays were upwards of 3 hours – but by the second week of disruptions, public transport trip times were close to normal.

Figure 6: Photo of a rail passenger shelter in the April 2019 city loop shutdown: it has capacity for queueing many thousand travellers, but smooth customer service kept waiting times below 10 minutes.

5 CONCLUSION

The tools of resilience engineering take a complexity view of real-world problems, seeking to understand boundaries and interfaces, adaptive cycles, and the mismatch between the system-as-designed and the real system. In contrast, the complicated problem-solving approach of conventional engineering focuses down and in to analyse component behaviour to assure inherent safety in a system-as-designed.

Worldwide, rail is struggling with the limits of the command-and-control perspective on safety and operations. Each step of technological advancement pushes the precursor to an accident further back in the design cycle, which increases the delay between cause and effect. Additionally, the interconnectedness of different technical and human systems couples their behaviour together through feedback loops. The fundamentals of complicated problem-solving - standards, central control and synoptic legibility – are being stretched to the limit.

The major benefit of a resilience engineering approach is that it lets engineers understand the real system, and closes the blind spots from focusing too deeply on the system as designed. Complex systems principles offer a way to understand and alter system behaviour through the use of feedback across boundaries, the adaptive cycle at different scales and timeframes, the understanding that a disruption is an opportunity to learn, experiment and see if a system element previously seen as a 'problem' can become an active part of the solution. This requires courage to be wrong, multi-disciplinary skill sets, and focusing upwards and outwards beyond traditional engineering system boundaries.

The author proposes that engineers need to be more curious about real world system behaviours, especially where there are contradictions or decay in practices compared to the system as designed. We should:

- Be persistent (even obnoxious) in enquiring and seeking information across boundaries,
- Skate across the high level big-picture and drill deep into the detail,
- Use feedback between systems of different scales /timeframes to report problems or trigger change,
- Always seek to improve communication and alignment between tightly coupled systems.

The increasing system complexity is inevitable, and the opportunity is now for railways in Australia and worldwide to step up to meet the challenge – before the megatrends threaten railways as a mode of transport with obsolescence.

6 REFERENCES

1. Hollnagel, E., Woods, D., Leveson, N. *Resilience Engineering*. Great Britain: Ashgate, 2006
2. Hollnagel, E. *Safety-I and Safety-II: The Past and Future of Safety Management.* Ashgate, 2014
3. Dekker, S. *The Safety Anarchist: Relying on Human Expertise and Innovation, Reducing Bureaucracy and Compliance.* Taylor & Francis Ltd, 2017
4. Reason, J. *Human Error*. UK: Cambridge University Press, 1990
5. Reason, J. *The Human Contribution*. USA: Ashgate, 2008
6. Almaberti, R. *Navigating Safety: Necessary Compromises and Trade-Offs - Theory and Practice.* Springer, 2013
7. Naím, M. *The end of power: from boardrooms to battlefields and churches to states, why being in charge isn't what it used to be.* USA: Basic Books, 2103.
8. Australian Government. Critical Infrastructure Resilience Strategy [Online] https://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf [18/05/19]
9. Melbourne rail network map, Public Transport Victoria [Online] https://www.ptv.vic.gov.au/assets/PDFs/Maps/Network-maps/0bc94c22f8/PTV_MetropolitanTrainNetworkMap_August2018.pdf [19/05/2019]
10. Taig, T. *Review of the Rail Industry Safety and Standards Board and its MOU with the Governments, June 2012* [Online] https://www.transportinfrastructurecouncil.gov.au/publications/files/RISSB_review_report.pdf [26/05/19]
11. Walker, B. and Salt, D. *Resilience Thinking – Sustaining Ecosystems and People in a Changing World.* USA: Island Press, 2006
12. Woodbridge, P. *A chronology of UK Railway Signalling, 1825-2018*. Peter Woodbridge, UK, 2018
13. Waugh, A. "Victorian Railway Maps, 1860-2000" [Online] http://www.vrhistory.com/VRMaps/ [26/05/2019]
14. Cowie, T. *Melbourne Metro train network goes into meltdown after computer failure* [Online] https://www.theage.com.au/national/victoria/melbourne-metro-train-network-goes-into-meltdown-after-computer-failure-20170713-gxarah.html [21/05/2019]
15. Carey, A . *Metro's $80m back-up system may have failed at moment Melbourne needed it.* [Online] https://www.theage.com.au/national/victoria/metros-80m-backup-system-may-have-failed-at-moment-melbourne-needed-it-20170714-gxbjs6.html [21/05/2019]
16. Jacks, T and Hope, Z. *No compensation for commuter peak-hour chaos* [Online]. https://www.abc.net.au/news/2017-09-01/metro-trains-fined-after-computer-glitch-caused-chaos/8862204 [12/05/2019].
17. Transport for NSW Bureau of Transport Statistics, *Train Statistics 2014 – Everything you need to know about Sydney Trains and NSW TrainLink.* [Online] https://www.transport.nsw.gov.au/sites/default/files/media/documents/2017/Train%20Statistics%202014.pdf [26/05/19]
18. Xinhua, *China's high-speed railway length to top 30,000 km in 2019* [Online] http://www.chinadaily.com.cn/a/201901/03/WS5c2d7755a310d91214053454.html [26/05/19]
19. Gao Ling. ATO Application for Inter-City Rail in China. *IRSE proceedings: ASPECT 2017.* Introductory Day - 27 November 2017.

20. Allday, S. Keynote Address: Sydney Metro Project. *IRSE Australasia National Technical Meeting,* 21 November 2018.

21. Carey, A . *State of growth: Victoria's $100 billion infrastructure boom revealed* [Online] https://www.theage.com.au/politics/victoria/state-of-growth-victoria-s-100-billion-infrastructure-boom-revealed-20180805-p4zvns.html

22. Andreevski, I. and Walker, M. 3D Signal Sighting Workflow. *IRSE Australasia National Technical Meeting,* 18 July 2019.

7 ACKNOWLEDGEMENTS

My deep thanks to my wonderful colleagues and the professional communities of signalling, systems engineering, safety and appreciative enquiry. Particularly Peter Woodbridge and the IRSE and SESA Victorian chapters.

Cherie Lee and John Dyer – thankyou for your input into this paper, and for working alongside me every day on high stakes multi-organisation multi-discipline rail-industry-specific change techniques we have been developing together. It has been so powerful to use the day job to transition an idea from research to real world practice.

Richard Stephens, I have had the privilege of thinking of you as the other half of my brain for some years now. Once again, it was a pleasure to have you alongside on this one. Extra thanks for your epic editing.

My last and biggest thanks to my family who understand that Mum gets a bit strange and grouchy when there is a paper deadline looming. Brendan, Isaac, Joseph and Amelia, you are my foundation. You have done this many times and know the rhythm of this work - but I am always grateful.