Moving the Mindset: from Safety to Systems Safety

Alistair Campbell & Zahid Qureshi
Defence and Systems Institute (DASI)
University of South Australia
Building F, Mawson Lakes campus
Mawson Lakes SA 5095, Australia
alistair.campbell@unisa.edu.au

Abstract: Safety is the focus when accidents occur, and the default approach among the experts deployed to investigate such safety incidents, is to concentrate on the technology issues or human errors in isolation. While specific technical faults or human errors can typically be identified as having initiated the safety breach, widening the focus to gain a more systemic understanding of the context within which the accident occurred, is increasingly being recognised as best-practice. Using the background of some important advances in the field of systems safety by authors such as Jackson and Leveson, this paper draws out the crucial role of the socio-technical aspects.

This discussion is then contextualised by using examples taken from railway safety case studies, to focus on some key practical implications of using this enterprise-wide systems approach. The paper concludes that a systems approach which includes the enterprise as well, becomes especially important when formulating strategic policy which works towards systems safety.

Introduction

In moving from safety in isolation to a more systemic view, it is helpful to consider some background on systems thinking, and compare it to the reductionist thinking that underpins much of the engineering and scientific endeavour that is so helpful in many other fields.

Reductionism

The reductionist thinking advanced by Descartes in 1637 (Descartes 1968) has allowed science to progress rapidly and impressively over the intervening centuries. Our present-day body of knowledge in a wide range of sciences is both impressive and crucially supports the technological and other advances that have improved our living standards by orders of magnitude, when compared to the 1600s. Just 100 years ago for instance, the typical speed limit was 10mph, life expectancy was below 50 years, and 9 out of 10 homes did not have a telephone. Reductionism has played a vital role in underpinning the scientific thinking and research behind most of the spectacular advances that have been made over the past several centuries.

However at the beginning of the 20th century the emergence of a new field of enquiry began to encounter the limits of reductionist thinking. This was the "new science" of quantum physics. The following quote (Capra 1989: 76) captures the change of thinking required:

> *Even after the mathematical formulation of quantum theory was completed, its conceptual framework was by no means easy to accept. Its effect on the physicists' view of reality was truly shattering. The new physics necessitated profound changes in concepts of space, time, matter, object, and cause and effect; and because these concepts are so fundamental to our way of experiencing the world, their transformation came as a great shock.*

Clearly reductionist thinking on which scientists had relied for centuries, was beginning to reach the limits of its capabilities as science progressed into the 20th century. Another quote helps put this in perspective: *the more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent (Capra 1996).*

Technology and Engineering which have applied so much of the physics and science theory, are particularly prone to accepting reductionism as the default thinking, for the very good reason that it has supported those endeavours over centuries. However, in order to apply those technological marvels within a social context in which people and organisations are inextricably involved, requires a wider worldview that will accommodate the full socio-technical system.

Some Literature on Systems Approaches

Systems Thinking thus emerged in the mid 20th century, partly as a holistic response to the increasing complexity and fragmentation within many scientific endeavours, and the applied sciences such as engineering and medicine that in turn put these into practice. It is especially in this interaction between theory and practice that systems thinking finds its place, and in this paper two main literature sources are particularly relevant. Michael C Jackson (2000) provides a broad overview of systems approaches, within the social context of people and how they are managed within teams and organisations. At the level of application (rather than theory), which arguably may be more important in the context of this paper, Nancy Leveson (2004) outlines a systems approach to accident modelling which is usefully inclusive of the views, methods and approaches from a wide range of authors. This will explored in more detail later in the paper.

Systems Thinking is widely accepted as having been the initiative of Boulding (1956) and von Bertalanffy (1960). This is a holistic worldview, in which (Hansen 1995):

- Wholes cannot be taken apart
- Every apparent whole can be understood only in the context of the larger whole containing it
- A whole is more than the sum of its parts

◀ ● ▶

Reductionist thinking on the other hand regards (whole) problems as divisible into as many parts as is required to understand each part, and relies on re-integrating the parts to make it possible to understand the whole problem. Thus a car's engine can be analysed by dismantling it until every component is understood, and piecing this together again will result in an understanding of the overall working of the machine. However, when not dealing with a machine, reductionism begins to break down.

Consider the baking of a cake. Once baked, it is impossible to separate it into its constituent parts. Also, before being baked, examining the eggs, flour or sugar on their own, will give little clue as to their mutual interaction during the baking process, and thus only tentative indications of the outcome of the process. Similarly when analysing people within socio-technical systems, these are clearly not simple machine-like situations, and reductionism is therefore much less appropriate. Systems approaches make sense in complex situations that typically surround safety and accident analyses, most importantly as they also include the context of the team and organisational systems within which safety is preserved (or in which an accident takes place).

The development of Systems Thinking can be understood by referring to Fig.1 which indicates the influence this holistic worldview had on Organisational Behaviour in the 1970s and 80s (also known then as Industrial Psychology). The textbooks of the time (e.g. Baron 1983) typically made much of the new-found systems worldview to understand an industrial world that was emerging from the era that had built the fortunes of machine-age entrepreneurs, typified in the likes of Henry Ford, into one where "understanding and managing the human side of work" (Baron 83) was coming into focus.

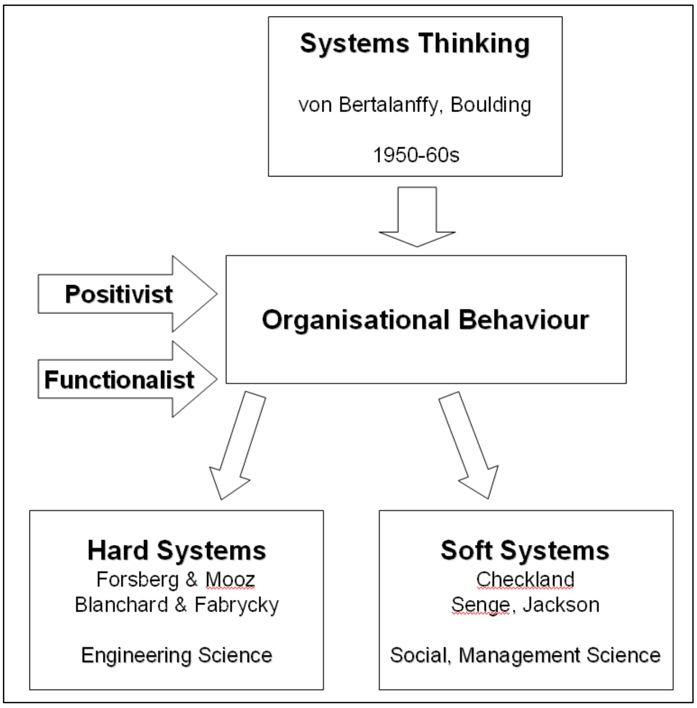

Fig.1: Development of Systems Approaches

The subsequent influences brought about by a resurgence of positivism and functionalism caused a split into the so-called hard and soft systems approaches. The hard systems approach can be typified by the now-ubiquitous V-diagram of Forsberg & Mooz and by the plethora of systems engineering methods and tools found in textbooks such as Blanchard & Fabrycky (1997). Hard systems approaches are therefore well aligned with the Engineering Sciences.

The so-called soft systems approaches are probably best characterised by the work of Checkland (1983) with the Soft Systems Methodology (SSM) still being among the best-known of these systemic approaches. Authors such as Senge, Jackson and others have added to this body of knowledge which can be classified as part of the Social and Management Sciences.

This paper is therefore concerned more with the right-hand side of Fig.1 in order to integrate the people-centric issues with those that are more technical in nature.

Jackson (2000) uses the depiction in Fig.2 to illustrate the progression that is typical in any piece of research. It begins with the theory framework (F) on the left, which is then embodied in the chosen methodology (M). This methodology is then applied in practice to the area of concern (A).

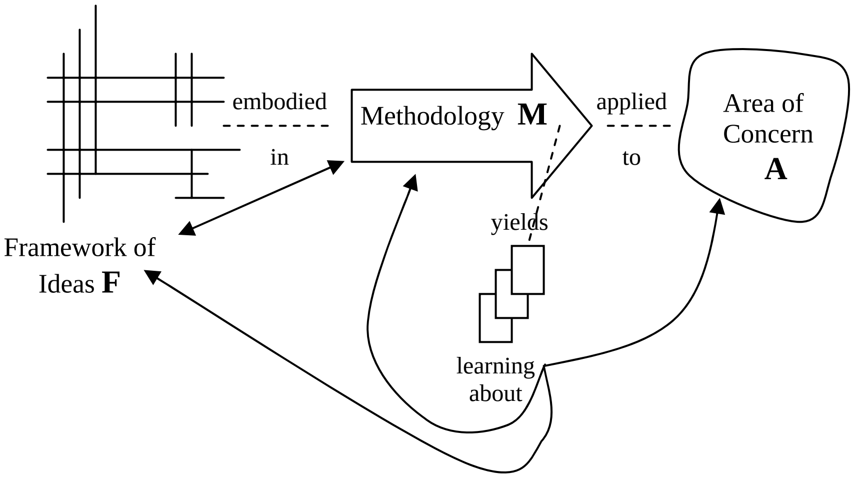

Fig.2: Progression of Levels: Theory → Practice *(Jackson 2000)*

In the context of systems safety and accident modelling, the methodology (M) is the accident analysis or safety investigation, and in most cases this also represents the method itself. The area of concern (A) becomes the accident finding (cause). In our case this needs to extend one step further to the right of Fig.2 to include the crucial recommendations and policies that will help improve future safety.

Returning to the left-most part of Fig.2 it is therefore clear that for a systemic approach to safety and accident modelling we need to ask what basic theory it is that we have chosen to underpin our analysis. Some suggest this choice of theory is implicit, maybe it is also unconscious, or sometimes even inadvertent. Perhaps we simply choose a method which seems to have worked in the past, and then begin to gather information, in what later turns out to be a largely reductionist way, expecting all the pieces to simply "come together" in the end, in a machine-like fashion.

The very different nature of systems approaches are for instance highlighted by observing that socio-technical systems involve people interacting with technology to deliver outcomes not achievable by either the technology or the people working alone. In a system it is not the elements that are most important but their interactions.

In the context of systems safety, Leveson (2004) sets out to develop a method of accident modelling with the express purpose of ensuring that the underlying theory relies on a systems worldview. From the discussion around Fig.2 it is clear that the theory which we choose to underpin our research or analysis, will have a profound effect on the way we develop the results of our investigation. Importantly, a systems approach will also have a fundamental influence on the ensuing recommendations or future policy initiatives.

In essence, Leveson's model, called STAMP (Systems-Theoretic Accident Model and Processes) takes the view that "system theory is a useful way to analyse accidents, particularly system accidents" (Leveson 2004:250). The method focuses on control of the system and the constraints that bring this about. An accident thus occurs when a safety constraint either breaks down or is absent, which can also be traced back to possible omissions in the design, or forward to a flaw in the through-life support of the system. The model builds on systemic concepts of control loops, process models, socio-technical levels of control, and the classification of accident factors. In this way the model applies the work of Ashby (1956), Rasmussen(1997), Checkland (1981), Leplat (1987) and other important authors in the field of systems theory and its application to the complex field of safety and accidents.

The Application of Systemic and Reductionist views

In accident investigations, the effect of reductionism can be quite subtle. This is because reductionist approaches (cause-and-effect, a chain of events, etc) do in fact result in an answer. However the answer we get is at a level that is, from a systemic point of view, at risk of being trivial. This is because when an answer looks only at who/what caused the accident, answering only what/who failed, the solution is then typically to ensure this item/person does not fail in future. It is not therefore immediately obvious that the reductionist answer is lacking in any way, since in one (isolated) sense, "the answer" has been identified.

To illustrate the contrast, take the problem of a common cold: when we treat a cold, we typically aim at the symptoms. Our blocked nose, stuffy sinuses, or headache are relieved by simple analgesic medicines, meanwhile our bodies do the real work of fighting the infection, and over time, mending our physical system. The "system answer" comes when our physical system is restored, although some might regard the relief of the symptoms as "the end of the problem", despite the sickness lingering within our body. One view is short-term, the other long-term; one is an isolated view of the symptoms, the other is a holistic view of our body as a system.

In the context of accident modelling, this draws attention to the contrast between reductionist (isolated) approaches and systemic approaches which account also for the Enterprise System within which accidents take place.

◀ ● ▶

Only when we include the human and organisational system in which the accident took place do we widen the system boundaries enough to capture sufficient complexity to be able to address the safety problem in a way that is both thorough and strategic. Importantly, policy initiatives based on an isolated view of "the answer" will be likely to result in what are typically later described as "unintended consequences". A systemic view however allows us the best chance at formulating policy in a way that accounts for the people, the technology, and the context of other factors within which they all interact.

Analysing a Railway Safety incident

To illustrate the differences between approaches that rely on reductionist thinking on the one hand and systems thinking on the other, we will examine an actual railway accident. It is in the recommendations and especially the policy implications that the differences emerge.

On 26 October 2005, the luxury passenger express, the Blue Train was ahead of time and diverted onto a passing loop at Deelfontein station to allow the regular long-distance passenger train coming from the opposite direction, to pass. As the passenger train approached the station at the cruising speed of 90km/h who could have known that the green signal in the dark South African night was in fact the result of a fault in the signalling system. The train was about to be diverted head-on into the stationary train on the track alongside. 74 people aboard the Blue Train and 183 travelling in the oncoming train were injured, fortunately only 5 were seriously injured and there were no fatalities.

In February of the following year, the independent board of enquiry released its report after an extensive safety investigation and hearings:

"It was established that the wrong-side signalling failure was as a result of a short circuit caused by a solder splatter in the relay unit".

It was determined that despite some visual inspection and electrical tests, the solder splatter remained undetected and therefore directly caused the malfunction of the relay unit, which eventually lead to a wrong side signalling failure that caused the collision between the trains.

Despite attempts by the driver to apply emergency brakes, it crashed into the Blue Train.

"The solder splatter was a 'trap', waiting for the occasion when the signal was set up in this particular way, to cause a wrong side failure," read the report.

The board of enquiry recommended that a comprehensive safety-management system audit be initiated by the Railway Safety Regulator to determine and rectify any deficiencies. It also recommended that Spoornet [railway organisation] review existing quality assurance measures to ascertain their reliability and extend the same to all contractors within the safety value chain. (Mail & Guardian 2006)
The signalling circuit improperly bridged by the solder splatter appears to have been single-switched. To prevent a recurrence, double switched circuits are proposed, also called secondary protection circuits. (RailwaysAfrica 2006).

As with most accident investigations this had a clear outcome. The train drivers were not at fault; it was the signalling equipment that had failed, due to a prior unforseen mishap – the solder splatter. The report also recommends a review of "the safety-management system" and "existing quality assurance measures".

The author (in a previous life) worked for the South African railways for many years, most of those spent as an engineer responsible for the final safety testing of the signalling system. The views that follow also utilise that experience to draw conclusions from the accident report.

It is hard to know from the accident report what approach the board of enquiry followed, either systemic or reductionist. However, the recommendations for the socio-technical organisation itself are somewhat lacking in focus, and do not seem to target a specific intervention. For instance, the suggested audit is a diagnostic tool rather than a remedial approach.
In stark contrast to this, the technical recommendation is quite clear: "to prevent a recurrence, double switched circuits are proposed". (see Note 1)
This contrasting clarity and then the lack of it, giving specific attention to the technical details but leaving a broad-brush statement to address the human and organisational systems of safety and quality, seems to indicate that technical aspects are primarily relied upon to address the safety issues. This strongly suggests that, in common with many engineering-based organisations, a reductionist approach was used during the accident investigation.

Let's now approach the accident from a systems perspective, and using systems terminology we widen the system boundaries to include the enterprise itself, namely the railways organisation, and the people within it. The general accident report does not mention any personnel other than the train driver, and this leaves a key question: how did the solder splatter get there? If we don't address that, it is unlikely we will be able to prevent a future occurrence.

The detail report states that the local technician worked on the signalling system at Deelfontein some time before the accident took place, using a soldering iron in the process. It is important in this analysis not to lay blame (Leveson 2004) but rather to objectively analyse and then draw systemic conclusions as to why it occurred – remembering that a socio-technical system consists of person and machine interacting – and then how to re-craft the system to reduce the likelihood of a reoccurrence.

The report also states that *despite some visual inspection and electrical tests, the solder splatter remained undetected and therefore directly caused the malfunction.* Any safety engineer would know that testing a (signalling) system for safety involves a lot more than "visual inspection and electrical tests" – quite simply, the equipment has to be tested as a system. Apparently this was not done. This is a serious failure of the safety system as a whole – and no amount of technical sophistication can circumvent the crucial requirement to have a competent person test the signalling system after it has been worked on. In Leveson's STAMP approach this is would be termed a system constraint that was not properly applied, leading to a loss of system control.

As is typical of most engineering technicians, railway technicians regularly attend to minor signalling faults and the use of a soldering iron is a normal occurrence. However, what is not normal is that the technician should be left to test the signalling system and certify its safety. This is the responsibility of the engineer assigned to that district – and it is the engineer who will have to demonstrate the system safety (and test procedure) in court in the event of an accident – and engineers typically guard this responsibility quite fiercely.

The crux of the accident failure from a systems point of view is therefore the failure of this socio-technical constraint. If it had been adhered to it is very likely that a system test would have detected the wrong-side signalling error, and in turn identified the solder splatter that was causing it – crucially, the slip would have been discovered before an accident could occur.

The systemic solution is therefore to uncover where in the organisation the safety testing is spelled out, and how it was circumvented in this case. An organisational and people-centred solution is thus to fix the safety breach at this crucial systems level (in addition to the technical). This might require restructuring parts of the organisation and in this regard authors like Mintzberg & Quinn, and Gareth Morgan (1997) identify a number of different organisational models. By choosing an appropriate model the organisational structures can then support the aims of safety in a way that regards the people, the enterprise and the technology as a system, instead of as stand-alone elements. In this way system safety is strategically designed-in as a property of the organisation as a system, rather than as an add-on feature.

Let's now examine the technical solution and assume for a moment that the "double-cut" circuit is introduced to this part of the equipment. Nothing prevents a new solder splatter from occurring on a different part of the circuity in future, or the occurrence of any number of electrical malfunctions due to bent wires, frayed insulation, or even a simple oversight by the skilled and well-intentioned maintenance technician. And any of these simple technical mistakes could potentially result in another similar accident. The technical "solution" in isolation will therefore result in little more than a marginal increase in system safety.

The safeguard is thus not to be found in the technology alone, since safety relies significantly on the system within which it operates. If the system malfunctions, and safety testing is not suitably constrained, it is unlikely that the technology by itself will be able to ensure a safe signalling system.

The systems approach therefore produces a very different safety recommendation: to fix the reporting structure within the organisation that supports signalling system safety testing. The main focus thus turns toward the integrity of the socio-technical enterprise system to ensure that each time the signalling system is worked on (the technology "in isolation") it is then tested as a system, by someone who is properly responsible for carrying out such system safety checks.

There are any number of reasons as to why, in this case study, the system constraint (system testing) was not upheld and the investigation should tease these out – again, not to apportion blame, but to reason through the systemic controls and discover where they are lacking. The reason may for instance be that the technician was called out to the original fault at 3am and didn't want to wake the engineer for "something trivial". It could be that a contractor was on site and the technician lost sight of, or was not informed of, the influence this might have on the equipment and its safety. Who knows?

Conclusions

Whatever the actual reason for the system-testing constraint breaking down in this case, when it comes to policy it is clear that the safety procedure needs to emphasise the critical and systemic nature of equipment testing, for future occurrences to be minimised.

So, while the reductionist approach has, somewhat predictably, focused on a technology solution, the systems approach has instead identified the breakdown of a system constraint, leading to a loss of control within the enterprise system. The socio-technical interaction is quite apparent in the systems view, and in contrast, almost entirely absent in the reductionist outcome.

Importantly, the advantage of the systems approach to safety and accident modelling is found especially in the resultant policy recommendations and actions. This can be illustrated by considering which option one would prefer, assuming one was planning on a train trip that passed through Deelfontein station. Would the technical solution alone, a double-cut circuit, provide sufficient confidence? Or would one prefer the systemic solution, knowing that a competent person within the organisation had certified the safety of the signalling system?

It is clear that the systems approach also includes the technology solution, but the point is, it goes further – addressing the whole socio-technical system on which safety depends.

Note: 1. This is a technical redesign of the specific circuit, which certainly reduces the risk, but statistically only by half, so to claim that it will "prevent a recurrence" is a bit of a bold statement, indicating again the reliance on technical solutions to "ensure" safety.

References

Baron, Robert A. et al 1983 *Behavior in organizations : understanding and managing the human side of work*. Allyn and Bacon, Boston, MA, USA.

Blanchard, Benjamin & Fabrycky, Wolter 1997 *Systems engineering and analysis* Prentice Hall, Upper Saddle River, NJ, USA

Capra, Fritjof 1989 *Uncommon Wisdom* HarperCollins Publishers.

Capra, Fritjof 1996 *The Web of Life: a new synthesis of mind and matter*. Flamingo, London.

Checkland, P 1981 *Systems Thinking, Systems Practice*. John Wiley & Sons, New York.

Descartes, René 1968 *Discourse on Method and the Meditations* translated by F.E. Sutciffe. Penguin Classics, Harmondsworth.

Leplat, J 1987 "Occupational accident research and systems approach" in: Rasmussen, J., Duncan, K., Leplat, J. (Eds.), *New Technology and Human Error*. John Wiley & Sons, New York, pp. 181–191.

Leveson, N 2004 "A new accident model for engineering safer systems" *Safety Science* Vol.42 pg.237-270

Mintzberg, Henry & Quinn, James Brian 1996 *The Strategy Process: Concepts, Contexts, Cases* Prentice Hall International, London.

Morgan, Gareth 1997 Images of Organisation Sage Publications, Thousand Oaks (CA), USA.

Rasmussen, J 1997 "Risk management in a dynamic society: a modelling problem" *Safety Science* Vol.27 pg.183-213.

Mail & Guardian archive report, 22 Feb ’06: "Signalling fault caused Blue Train crash", accessed at www.mg.co.za on 20 June 2008.

RailwaysAfrica Issue 1/2006 referenced by Wikipedia entry: "2005 Deelfontein train collision" accessed 20 June 2008.

Wikipedia entry: "2005 Deelfontein train collision" accessed 20 June 2008.

Biography

Alistair Campbell has a background in both Engineering and Business, and a career that consists of roughly equal periods in industry and academia. Initial years were spent in project management of railway traffic safety systems, before branching out into his own business for several years. In 1992 he joined the Cape Peninsula University of Technology, Cape Town, and left there in 2005 to join the University of South Australia. He has a Bachelors degree in engineering from the University of Stellenbosch, a Masters in Business Leadership from the University of South Africa, and a PhD from the AGSE at Swinburne University of Technology in Australia. His research interests include: Applications of Systems Thinking, Innovation & Entrepreneurial Strategy, Human Dynamics in New Ventures, and Renewable Energy Systems.