Bexley train crash – a system failure

By Dr Chris Elliott MBE FREng

Executive summary: A goods train derailed with three independent causes: poor track maintenance, overloaded wagons, and excess speed. The "holes in the Swiss cheese" lined up, and each hole had many complex underlying causes. Safety of a complex system must be planned and executed as a system, not as separate pieces.

Tags: train derailment, train accident, transport, root cause analysis, accident inquiry, inadequate resources, contractual complexity, political priorities, systematic planning, United Kingdom.

Section 1: Background and introduction

On 4 February 1997 a goods train derailed at Bexley. Four people were seriously injured and there was extensive damage. HSE investigated the accident[1] and subsequently prosecuted the track owner, operator and maintainer (Railtrack and its contractor) and the train operator.

The accident is informative because it had three immediate causes and it is likely that all three were necessary for the accident to happen.

1. Poor track maintenance: the longitudinal timbers supporting the track on the bridge were rotten, allowing the rails to move ('gauge spreading')
2. Overload: the wagon that derailed was estimated to be 30% over the permitted weight for a line rated for the heaviest loads (RA10); this line was rated below that (RA8).
3. Overspeed: the inquiry did not estimate the impact of the overspeed of around 37% but it is reasonable to assume that the dynamic loads are at least proportional to speed so the dynamic effect was as great as the static overload.

However, the chain of causation is more complex because each immediate cause had root causes:

Maintenance

- Railtrack (principal duty-holder) had failed to follow its audit plan
- SEIMCL (maintenance contractor) had not communicated well with Railtrack
- There was major restructuring of staff in SEIMCL and a critical post was vacant
- The condition of the sleepers was so poor that they could not have decayed to that state within the three years since Railtrack inherited responsibility, they must have already been defective when maintained by British Rail

Overload

- The wagons had carried ballast, less dense than the spoil carried on this day
- The loaders were told to use only 75% of the volume of the wagon, without any justification for that value.

Overspeed

- The speedometers in the cabs were under-reading by ~ 10%
- The driver was not aware of the local rule regarding the speed of goods vehicles (which was lower than the 'signed' speed)
- The driver had been trained at a centre that systematically did not teach this rule.

Section 2: Analysis and insights

At its simplest level, this is a classic system failure. It is well described by Reason's 'Swiss cheese' model in which holes in three layers of protection (track maintenance, load control and speed control) lined up to allow the accident to occur. Many trains had passed over that section of track without derailing, it is likely that some were overloaded and that some were speeding, but a train that combined all three elements caused a structural failure.

It also illustrates the error of latching on to the immediate causes. All three had deeper root causes that reflected failures of management systems. The contractual arrangements for track maintenance were complex and badly defined, with inadequate resources and poor information flow. The loaders were poorly instructed and the system for instructing them was inadequate, with inadequate review and quality control. There was no control on speedometers and there was a long-standing failure to train

Royal Academy of Engineering
LR Foundation

drivers of freight trains in the rules across all parts of the network. The inquiry also found other safety failings, such as the incorrect tare weight on one of the wagons, but concluded that these did not contribute to the accident.

The contractual complexity is illustrated by the train itself – the wagon that started the derailment was owned by CAIB UK Ltd and operated by English, Welsh & Scottish Railways Ltd and the driver was on contract from Connex South Central.

A complex contractual chain (or more accurately network) is not intrinsically unsafe – civil aviation has a very complex contractual structure without compromising safety. However, it demands proper planning, adequate resources and especially very careful management of the transition from a simple integrated regime to a fragmented regime bound together by contracts. All three were absent in the transition from vertically-integrated British Rail to the fragmented privatised railway.

The over-riding message is that successful safety management of a complex system must be planned and executed as a system, not as a set of separate measures.

Section 3: Discussion and transferable learnings

This case study illustrates the issues outlined by the York Framework[2], depicted in **Figure 1**, previously released by the Safer Complex Systems mission:

Causes of system complexity

- Railways are intrinsically complex and rely for safe operation on clear and unambiguous rules that are strictly followed
- The railway had been broken into many independent companies
- Regulatory structures were weak, relying on duty-holders without close oversight
- Technical complexity is easily recognised, management complexity is not

Consequences of system complexity

- No one person 'owned' the issues
- Unsound practices were allowed to persist

Design-time controls

- Track speed and loading ratings were not known or enforced
- No procedure existed to verify speedometers, or if it did, it was not followed
- Decisions were arbitrary and not subject to review
- Audits were not conducted

Operation-time controls

- Key staff (loaders, drivers, maintenance planners) were not properly briefed
- Inadequately-trained drivers were used

Exacerbating factors

- General sense of confusion following the definition and implementation of the fragmentation of the railway
- Failure to replace previous informal practices that relied on personal relationships with a systematic safety management system

This accident raises many wider issues because it can be used to shine a light on some of the problems that the UK's legal system has when dealing with system issues.

Criminal law

The test of criminal liability is that the defendant did, and in most cases also intended to do, the act 'beyond reasonable doubt'. In this case, it is hard to see any doubt that all three of the failures (maintenance, overload and speed) passed this test but only two were prosecuted. Arguably the one that was not prosecuted (speed) is the most serious because it was systematic and long-standing.

The test in the Health and Safety at Work Act is that the defendant did everything reasonable to reduce risk (ALARP). This is a powerful and elegant rule but struggles with statistical causes and frequently uses an irrational concept of 'reasonable'. In this case, it may not have been reasonable for the duty-holders to have put right the flaws in their systems, even

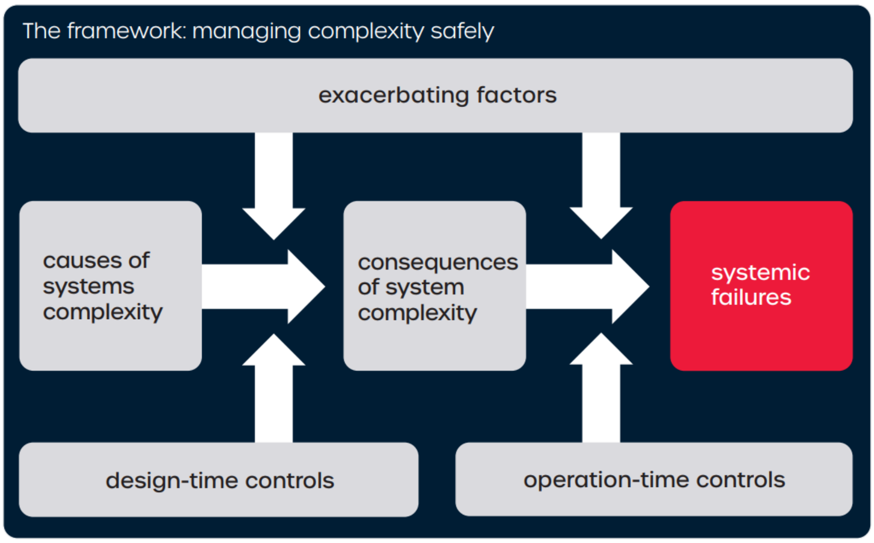

Figure 1: The York Framework[2].

though they are obvious with hindsight, if they were driven by political pressures and constraints and had inherited a backlog of maintenance and lack of management systems from a quite different legal structure.

Although railways rely on strictly following rules, it is impossible to encode those rules in a legal framework, which will always lag behind innovation in practices and technology. This accident occurred before rail regulation adopted the 'New Approach' of general legal principles and industry-made detailed rules. After around 30 years of successfully applying this approach, there are disturbing signs of returning to a prescriptive regime, for example for autonomous road vehicles

Health and safety law in the UK is largely based on the seminal report of the committee chaired by Lord Robens in 1972. That report argued that complicated prescriptive standards should be replaced by a duty on each employer to strive to eliminate risks to workers and others, so far as is reasonably practicable. However, the report states in paragraph 182:

> *We accept that transport safety is a vast study in its own right, involving many technical problems of a highly-specialised nature. Provisions for the safety and health of those engaged in flying aircraft, driving trains, lorries and so on clearly cannot be considered in isolation from a whole complex of special considerations such as the constraints imposed by the design of transport vehicles; the circumstances in which they operate which include many eventualities beyond the control of an employer; and the predominant need – in terms of numbers at risk – to safeguard the travelling public and the public generally. We accept that these matters must be dealt with within transport legislation.*

Paragraph 475 of the report summarises the conclusion:

> *The legislation .. should not apply to the normal use of the highway, to domestic service, or to transport workers whilst actually engaged in transport operations.*

Lord Robens and his committee understood that it was not appropriate to hold one person to account for failures of a system over which he does not have control.

Despite Lord Robens' clear statement, the consequent HSWA is applied to systems. Also the UK is unusual in that it is underpinned by criminal, not civil law.

That is fine when the breach is simple and obvious. If an employer does not give his staff adequate Personal Protective Equipment for work in a hazardous environment, he is guilty unless he can prove that it was not reasonably practicable to have done more. It is much harder to enforce when the harm is an emergent property of the action of many employers: A + B → C

Attempts to reconcile the criminal legal system with the word 'reasonable' have led to several other distortions that may be particularly unjust when applied to system failures:

- using ill-defined concepts like 'gross disproportion'
- in a complete inversion of normal legal logic, arguing that a breach may be serious enough to constitute a crime but not serious enough to constitute a tort/civil wrong
- placing the onus of proving that an alternative was not reasonably practicable on the defendant, thus creating a presumption of guilt until proven innocent.

Conclusion: The UK's safety law, including HSWA, was never intended to, and is poorly constructed to, apply to systems

Civil law

Tort law relies on the concept of causation – this requires that the outcome should be sufficiently proximate to an action for that action to be causal. Where the evidence is only statistical, an event must be more than 50% likely to have been the cause for causation to be found. Where three immediate causes together led to an accident, it is arguable that none contributed more than 33% so there is no causation. In a 2006 paper[3] the present author wrote:

> *But what happens when the risk arises solely from the interaction of the parts of the system. You can't then apportion the risk to each part – it makes no more sense than to try to describe the sound of one hand clapping.*

The tortious principle of causation has many weaknesses when applied to complex failures, especially when there are known and unknown unknowns and when it has to deal with the apportionment of risk. The principle is that there is no liability unless the failure is more than 50% likely to have caused the harm – there is no allowance for loss of expectation value.

If liability arises, it is for the condition of the victim at the time, not for the condition of a normal victim (known as the egg shell skull). Although this was not a consideration here, all three of the causes had 'egg-shell' conditions unknown to the other players.

Civil liability is determined on a balance of probabilities, which is hard to determine in a three-cause event.

Civil liability often hinges on the question of whether the victim would have suffered 'but for' the defendant's actions. This accident illustrates the difficulty of applying the 'but for test' in a system failure.

Contract law is better on probability but is still challenged by causation.

Conclusion: Civil law is poorly constructed to apply to systems.

Accident investigation

This accident was investigated by HSE, which then prosecuted two of the companies that it investigated. Since then rail accidents have been investigated by the Rail Accident Investigation Branch. RAIB's website states 'Our investigations are focused solely on improving safety. We are not a prosecuting body and do not apportion blame or liability.' However, legal protections for witnesses are weaker than for the Air and Marine equivalent bodies, an essential feature of the success of their impact on safety.

Two fundamental tools to improve the safety of systems are: confidential but not anonymous reporting of accidents and incidents; and impartial expert investigation after an accident to find the root cause.

Both depend on a willingness to be open and share knowledge and experiences without fear of recrimination, within a 'just culture'. The concept is best developed in transport. The three bodies in the UK that investigate transport accidents have an overriding duty to identify causes, not blame. Air and maritime investigations have legal protections that ensure that their reports and opinions may not be used in legal proceedings concerned with blame or liability. Rail reports may be admitted to such proceedings but the statements on which they draw remain confidential. Witnesses may therefore safely cooperate with the investigators in the knowledge that they will not be incriminating themselves or, even if they are not culpable, providing ammunition for opportunist civil legal actions in negligence.

These protections are constantly under threat by the need to attribute blame. Why do we investigate accidents: to prevent them recurring or to identify and punish the guilty?

Conclusion: Impartial, non-judgemental investigation has proved invaluable for transport safety and needs to be generalised to all complex system failures.

References

1. ISBN 0 7176 1658 4, 1999
2. McDermid et al, 'Safer Complex Systems: An Initial Framework', Engineering X, 2020
3. Elliott, 'Systems and the law', IET 1st Intl Conf on System Safety Engineering, 2006

Acknowledgements

This work was supported by a grant from the Safer Complex Systems mission of Engineering X, an international collaboration founded by the Royal Academy of Engineering (the Academy) and Lloyd's Register Foundation (LRF). The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Academy or LRF.

Affiliations

Dr. Chris Elliott MBE FREng, Director, Pitchill Consulting