A whole-railway reliability approach to planning for things that will probably never happen

Eur Ing Andrew Love, MEng(Hons) MA(Cantab) CEng MIET MIRSE, SNC-Lavalin Atkins

SUMMARY

Many railways understandably focus their attention on improving safety and reliability into eliminating the causes of the most commonly experienced incidents. However, this approach neglects the mitigation of low-probability high-impact incidents that might only be experienced once in the life of a transit network, but would be significant (potentially catastrophic) should they occur, such as wide-scale power or communication failures and earthquakes. Although such risks exist throughout (and beyond) the railway system, the role of communications, telemetry and operational control in mitigating or managing the impact of such risks means that addressing these issues falls squarely into the remit of the IRSE's members.

This paper considers the nature of these vulnerabilities, and how they can be identified, and mitigated.

1 INTRODUCTION

In this paper, I will discuss:

- The need for a structured, quantitative approach to identifying and assessing potential threats, so that an appropriate level of attention is given to mitigating low-probability events.
- The use of a whole-railway resilience model to identify risk mitigations from the human components of the railway system and dependencies from interfaces from outside the railway systems, as well as the more obvious risks and mitigations from the technological components of the railway system.
- The importance of assessing the environment in which the railway operates.
- Examples of how the impact of low-probability failures can be designed out or mitigated
- How railways can test their resilience to ensure that mitigations are effectively implemented.

It would be inappropriate to name many of the examples of resilience facilities in this paper; infrastructure owners are understandably guarded about their levels of resilience and such information could be of use to miscreants.

2 UNDERSTANDING THE PROBABILITY/IMPACT LANDSCAPE

2.1 The probability/impact curve

The relationship between probability of an event and the impact of an event can be plotted on a probability/impact curve, also known as an F/N curve. The events are typically derived from HAZID studies (and previous experience) followed by risk assessment to identify the probability and impact. These typically have a characteristic shape which I have approximated on Figure 1.

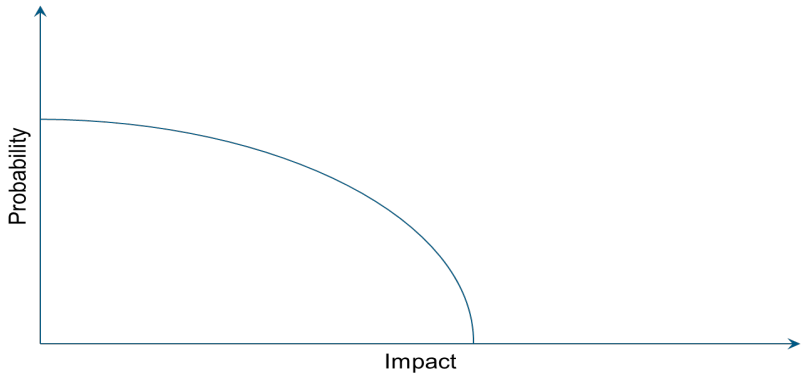

Figure 1: A typical railway systems probability/impact curve

However, these risk identification techniques may fail to identify two categories of hazard:

- **unnoticed** or **unmeasured** events, which are very common but of low perceived significance, and may not be noticed unless they are actively being searched for.
- "**unexampled**" and "**unimagined**" events. "A Typology of Resilience Situations" (Westrum, 2006) defined "unexampled" events to include events which could not be imagined as well as events which had never happened – I have used more explicit terminology.

Adding these categories of events to the probability/impact curve gives the modified form shown in Figure 2:

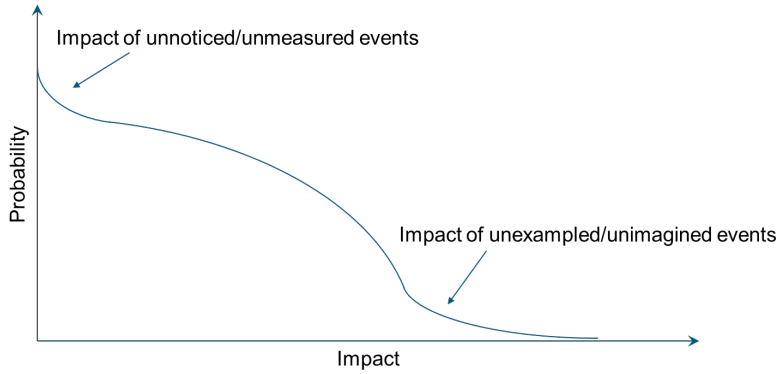

Figure 2: A railway systems probability/impact curve including missed events

I have split this curve into four zones as shown in figure 3. These are:

- Inconsistency, where imperceptible changes in how the railway performs (e.g. runtimes, reaction times) cause detriment to the overall performance of the railway
- Perturbation, where small but noticeable events (e.g. a passenger holding a door for a friend) cause a detriment that might appear trivial without further analysis, but which can combine to cause measurable impact on the overall performance of the railway.
- Unreliability, where the failure of systems and processes to work as planned causes measurable impact on the overall performance of the railway.
- Vulnerability, where there is a possibility that a significant event will occur, but it is treated as a one-off event. As probability decreases, it is tempting to think of such events as bad luck rather than to actively prevent or mitigate them, and these hazards are sometimes discarded prior to full analysis. However, the risk level of the event (probability multiplied by impact) may still be similar to that of other events in the more moderate probability/impact region, so it is rational that it should be afforded the same attention as more typical events. At the tail end of the curve are events that might not happen in the life of the railway system – but if they did, they would be devastating.

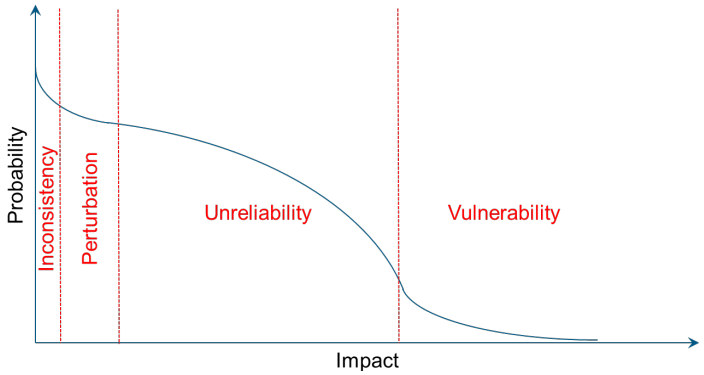

Figure 3: Zones of the railway system probability/impact curve

This paper focusses on these high impact, low probability events in the "vulnerability" zone. This should be "home territory" for signalling engineers who are (or should be) taught to identify and mitigate unlikely events when designing train control systems – but in this paper I will be applying this thinking at a whole railway level

2.2 National Risk Models

The first duty of government is to protect the people, and one of the means in which this is achieved is by governments assessing the risks which face their nation so that mitigation can be undertaken by the government itself, by organisations and by individuals. The risks identified by these initiatives are not railway-specific, but can form a useful resource to help identify low-probability high impact risks.

In the UK, the Cabinet Office maintains a detailed National Risk Assessment (which is classified), but publishes a summary where specific risks have been grouped as the National Risk Register of Civil Emergencies. This in turn drives documents such as the National Business Resilience Planning Assumptions, as well as frameworks for national, regional and sector-based response to incidents.

The 2017 UK National Risk Register summarises the threat to the UK in two risk matrices, one covering UK hazards, diseases and societal risks (figure 4) and the other covering UK malicious attack risks (figure 5). Some interpretation of the results is required, as the probability and impact category definitions have not been published and there is some overlap and consequential interplay between different groupings. The probability and impact are also rated for the general population rather than for railways, so the impact of (for example) power grid disruption would be more significant for the users of an underground railway than for the population in general.

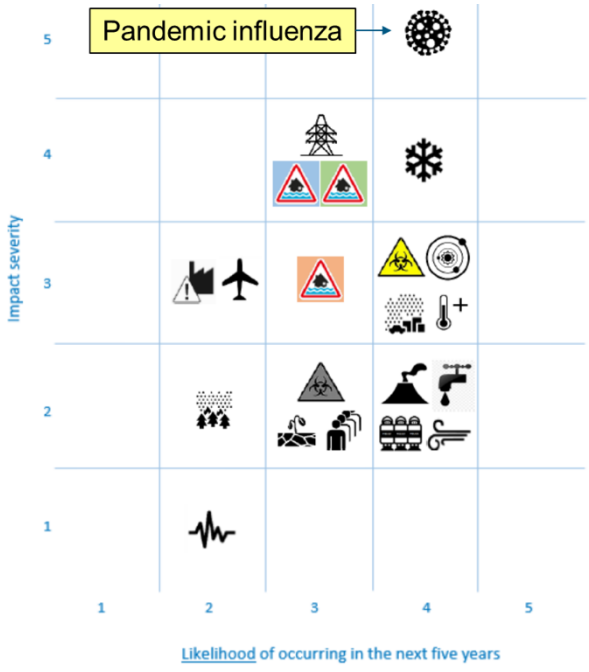

Figure 4: UK hazards, diseases, accidents & societal risks

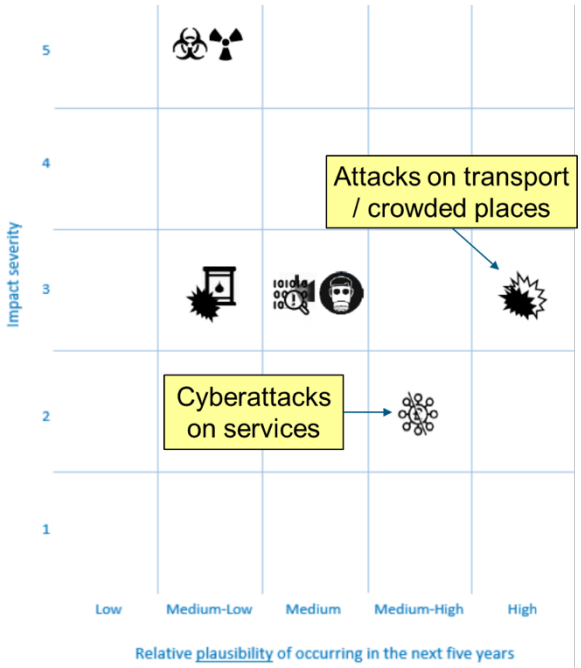

Figure 5: UK malicious attack risks

Figure 4 shows that the risk with the highest overall rating (probability multiplied by impact) is pandemic flu; I have therefore used this as an example of railway impact in the next section. Figure 5 shows no threats that are rated with both high plausibility and high impact. It does shows "attacks on transport and crowded places" as high plausibility, and cyberattacks on services as medium-high plausibility; sadly, both of these have happened since this report was published in 2017.

2.2.1 Example – Pandemic flu

The National Risk Register 2017 and National Business Resilience Planning Assumptions 2015 assume that in the event of an outbreak of pandemic flu:

- up to 50% of the UK population would experience symptoms
- 15 – 20% absence rates in the peak fortnight of pandemic (small / specialised teams should plan for 30% staff absence, and this rises to 50% if staff have caring responsibilities)

- fatality of 0.03% - 1.13% of the population might occur
- Supply chain disruption will occur if international borders are closed.

This will not only impact directly employed railway staff but suppliers and sub-suppliers; lack of performance from suppliers due to staff shortages is inevitable.

Staff with caring responsibilities may need to take time off work even while well – it is not clear how the suggested value of 50% reflects the impact of school closures on parents attending work, or even the impact of people who have suffered bereavement. There is also the risk that staff will stay away from work for fear of becoming infected, or due to difficulties in travel or other logistics caused by the pandemic.

How can the impact of this disruption in railways be mitigated?

Train operation: There are clearly benefits in fully automatic train driving (GoA4) as this reduces the dependency on train driver ability in normal operation. However, there needs to be sufficient competent staff available to recover failed trains (including a full system failure) within an acceptable timescale at all times that trains are in passenger service, so this solution does not give full mitigation from a loss of staff. Solutions such as remote train operation in the event of a failure would allow a greater number of trains to operate for a fixed number of staff, although this technology does not mitigate all failure modes.

Station operation: Many railways around the world are demanning stations and using SCADA technologies for remote operation. As with train operation, staff teams need to be available to deal with degraded conditions (whether misbehaving assets or misbehaving passengers!) but a reduction in staffing is achievable. Having moved the operation of assets, response to help point activations, provision of information and monitoring of security systems to the service control centre, it may be possible to move this further – see below.

Service Control: Increased automation at service control facilities (from basic Automatic Route Setting (ARS) to cutting-edge Traffic Management solutions) has reduced the staffing required to operate a train service, but has increased the impact of a member of staff being unavailable. Typically, simple ARS systems drastically reduce the staffing requirement for regular operation but fail to maintain this reduction during degraded mode operation; the more strategic approach of Traffic Management systems allows greater reduction during degraded modes of operation. The ability to dynamically allocate control of areas of the railway to different workstations (rather than having fixed areas of control) greatly assists the operation of a railway when fewer staff than ideal are available.

With modern IP-based control systems and good quality broadband links to people's homes, I believe that we have reached the age where some service control staff can work from home – this can maintain productivity of staff who are unable to travel to work or wish to avoid cross-infection but are otherwise fit to work. I do not believe that the control room of all but the simplest railways can be completely demanned – the ability to carry out a safe evacuation in the event of a major failure or incident needs to be safeguarded – but many activities can be supported by staff off-site with appropriately resilient arrangements. These might include passenger information (responding to station/train help point calls, providing audio/visual information on stations and trains), planning real-time service optimisations, and monitoring CCTV. There are already products which provide "Control Centre as a Service" (i.e. through a web browser) in use on some US railroads. A new control centre subsystem will be required to monitor the availability of remote staff (e.g. are they still connected?) and to enable real-time communication between site-based and remote staff as if they were still in the same room – similar to solutions developed by the online multiplayer gaming industry which allow gamers to communicate in real-time.

Clearly this mode of working would need to be thoroughly tested prior to a pandemic, but a remaining unknown will be how public broadband infrastructure reacts to a large shift to home working during an epidemic – non-business broadband links are "contended" so the data rate drops as more people use the infrastructure. There are technologies that can mitigate this for operational control purposes (e.g. constant latency CCTV) but there will come a point where network congestion prevents effective remote service control.

Maintenance: There will be elements of the maintenance function that can be carried out off-site, ranging from maintenance scheduling to technical support for technicians in the field and remote diagnostics; this will require access to asset database, asset documentation and diagnostic systems – clearly there are significant cybersecurity risks that will need to be mitigated for this level of remote access.

If insufficient staff or materials are available to carry out routine maintenance, these activities would need to be prioritised, and risk assessment would be required to demonstrate that the railway remains safe despite the changes to maintenance schedules. A key technology to assist this would be remote condition monitoring; this would give confidence that assets were not outside acceptable operational parameters, and would allow the available resource to be focussed on maintaining the assets which are closest to failing. Note that there may be increased station and rolling stock maintenance requirements during a pandemic – passenger and staff-facing surfaces will require regular sanitisation to reduce disease transmission.

When failures do occur, the use of redundant systems will reduce the probability of service disruption even if the fault cannot be immediately rectified, either due to lack of staff or lack of spares. To reduce the probability of running out of spares, the stockholding strategy should be reviewed to identify the impact of suppliers failing to deliver, particularly if international borders are closed. This will indicate where stockholdings need to be increased, or if this is not practicable, from where spares can alternatively be sourced – this might potentially be a lightly-used branch of the railway which will be suspended when required and used as a "donor" to provide spares for the remainder of the network.

With all of the above roles, additional resilience can be provided through:

- Cross-skilling staff, so that staff can be flexibly deployed to use whichever skillset is most needed
- Commonality of systems and processes, so that fewer skillsets are required to operate the entire railway and there is a greater pool of resource competent in each skillset.
- Prevention of infection by providing immunisation and heath advice for staff (and potentially for their family, to minimise the probability of staff absence due to caring responsibilities). Cross-infection at work can also be minimised by sanitising and compartmentalising the workplace.
- Support for caring responsibilities (e.g. a railway-sponsored playgroup if schools are closed)
- Training staff in personal resilience so they are less likely to miss work through personal misfortune.
- Ensuring that there is an adequate means for staff to indicate their availability for work and for suppliers to indicate their ability to deliver in real-time – this will enable effective planning to offer the best service possible for the resources available.
- Alternative suppliers – not just for point motors and signal lamps, but also for transport, catering and cleaning.

All of these changes to the normal modes of operation would need to be risk-assessed, in some cases prior to the pandemic as railways change their assets and processes to become more resilient, and in other cases, in real-time as processes are adapted (under a controlled process) to meet specific scenarios. This means that railways need to have appropriate processes and training so that effective real-time risk assessment can be undertaken, and there is an understanding of acceptable levels of risk in unusual times so that the railway neither closes its doors prematurely, unwittingly creating a greater societal risk, nor remains operating at an unacceptable level of risk when other, safer transport options are available.

Finally, it should be remembered that the pandemic will significantly affect passenger demand as well. There is likely to be a reduction in ridership as passengers will also be staying away from work and social activities for the same reasons as staff are unavailable; there might be opportunities to modify service patterns to enable the limited service capability to match the limited demand. It might be that some routes take on a strategic importance (e.g. to replace other transport modes that cannot be kept available, or to ensure access to healthcare facilities) or are used by the public to move from regions where the pandemic is more active to safer regions (hopefully not taking the disease with them!) The rail control system can facilitate these changes through dynamic timetable replanning tools and real-time staff rostering (e.g. crew management) tools.

2.3 Constant evolution of hazards

Hazards that drive high impact low probability events tends to change unnoticed; we usually see a change in risk profile through a change in the nature and severity of events, but these hazards generate very few events. They might change not just because of changes to a railway's own technologies, processes and ridership, but also because of evolving threats in the global environment, including geopolitical, meteorological, technological,

medical, commercial and social issues. The two most commonly discussed examples of this are climate change and cybersecurity.

Railways are experiencing weather events beyond their design assumptions. As one commentator asked, “Why do we now have a 1-in-100 years flooding event every 5 years?” Railways are now having to reconsider their approaches to track drainage (or at least their use of track circuits), their approach to stormwater attenuation, and the location of equipment rooms, substations and control centres using new meteorological assumptions.

Cybersecurity threats evolve as those who would gain access to our infrastructure learn more about the weaknesses in our software, hardware and processes and try to exploit those weaknesses. A system which was considered secure one day can be rendered insecure the next day by someone having a new idea on how to attack it. Railway operators must therefore remain aware of this changing landscape; as well as compliance with standards and applying manufacturer’s updates, regular penetration tests using ethical hackers are an effective means of seeing if changes to known techniques have compromised system security.

Identifying how a railway can be made more resilient through identifying the “unexampled” risks, developing mitigations and implementing these through changes to infrastructure, training and processes must be a continual process, not a one-time activity.

3 WHOLE-RAILWAY RESILIENCE

3.1 The whole-railway resilience model

A railway is a socio-technical system, comprising not only the engineering assets but the human resources and the processes by which those resources interact with the engineering assets to provide a passenger service. It is also subject to interfaces with an external environment (e.g. utilities, security) which can compromise its operation. When considering resilience of a railway system, it is appropriate to consider how diversity can be provided by assets, resources and processes, rather than the narrower definition typically used for reliability analysis which only considers the ability of an asset (or system of assets) to perform a given function.

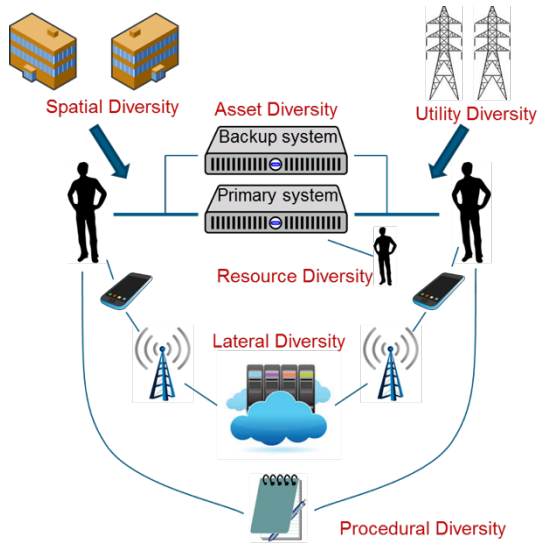

Figure 6: A whole-railway system resilience model

To investigate the resilience of the whole railway system, a diagram of the sociotechnical railway system has been drawn (see Figure 6) showing the possible types of diversity which contribute to resilience. This diagram uses the example of two members of railway staff communicating through a technical system (e.g. telephone, radio) as a sample function; the default path for communication is shown with a thick line, and a range of ways in which that communication could be diversely achieved is shown in thinner lines.
This figure defines:

- **Asset diversity:** this is the provision of resilience by replicating an engineering asset with a system which can perform the same function; for example a backup server or a duplicated communications bearer.
- **Utility diversity:** this is the provision of resilience through the provision of diversity in the utilities upon which the primary system is reliant, such as power, communications, or cooling. Examples include the provision of power supplies from multiple sources, the provision of additional air-cooling plant so that adequate cooling can be provided without 100% of the plant running, or the provision of multiple communications links.
- **Spatial diversity:** this is the provision of resilience through the location of equipment or resources in multiple locations so that unavailability of one location does not deny the availability of all equipment or resources. Examples include backup control centres, emergency stores and off-site copies of data and records.
- **Resource diversity:** this is the provision of resilience through having multiple members of staff which can perform the same function. For example, if one resource becomes unavailable to perform a function (e.g. a member of station staff being injured / distracted / experiencing radio failure), another member of staff with the same capabilities can be called upon to perform the required function.
- **Lateral diversity:** this is the provision of resilience through a different set of subsystems to those comprising by the primary system. Even if such a system has lower availability than the primary system, it can bring overall system benefits providing that there are no common points of failure. Lateral diversity is particularly effective at mitigating failures caused by unauthorised access to systems, as the means of access could form a common mode of failure for systems with asset diversity, but laterally diverse systems would have to be individually compromised, which is significantly less probable. Examples include the "COMPASS" degraded mode signalling system under development on the UK mainline network to provide basic train tracking using GPS when the primary signalling system is unavailable.
- **Procedural diversity:** this is the provision of resilience through carrying out a function using a procedure to mitigate the failure of a primary system, for example by driving trains manually following ATC failure. It is likely that such a solution will cause a significant loss in system performance but will allow the system to be placed into a safe state following failure of multiple subsystems.

Using these terms as a checklist when identifying mitigations to hazards ensures that the full range of possible mitigations is considered, instead of simply considering asset diversity. Significant further work could be expended in refining these definitions, but this is not required for the purpose of considering a range of options.

This model helps to raise the approach to resilience from being asset-focused (e.g. "Do we need a backup control room?") to being enterprise-focussed (e.g. "How will we cope if the control room becomes unavailable?") to enable a more holistic approach to planning and investment. Some of the non-asset forms of diversity can be surprisingly inexpensive and easily implementable compared to asset diversity.

Some of the forms of diversity, particularly resource diversity and procedural diversity probably already happen on the majority of railways without the railway operators having a term for it. It is valuable to identify these hidden forms of diversity, as this awareness prevents them being compromised through organisation change leading to loss of corporate memory, reduction in staffing levels, or introduction of remote-control systems.

3.1.1 How much resilience is appropriate?

It is possible to use these techniques to elevate a railway to a very high level of resilience, with sufficient effort and expense. There will be compelling (purely financial) business cases for well-targeted resilience against low probability high impact events even if the railway is not systemically critical to its environment. There are also societal requirements for resilience depending on each railways' systemic importance to their environment:

- Some railways are critical to the operation of a major city and will cause significant disruption (e.g. loss of economic output) if they are not available. Due to the sheer number of people who use them and existing congestion on streets, the provision of replacement forms of transport is infeasible.

- Other railways are beneficial to their environment (e.g. reducing journey time, improving journey quality and consistency, reducing pollution) but can be feasibly replaced by other transport modes (e.g. buses) with tolerable passenger impact.

Note that in some circumstances, the systemic importance of a railway changes in times of wider societal disruption; for example:

- if there are fuel shortages, a railway will see a surge in demand from people unable to drive to work
- in a regional evacuation, a railway might be the most effective means of transporting people quickly.

4 PRACTICAL RESILIENCE

4.1 How resilience should not be achieved

"Don't worry – we're got a backup control centre!" is a phrase that always fails to reassure me. While having a backup control centre is always going to give more options than not having a backup control centre, it is far from a panacea for every scenario, yet infrastructure owners still regularly think that by providing a backup control centre they have miraculously insulated themselves from everything which could disable their main control facility and hence thought no more about it.

Typical issues that get missed include:

- How will competent staff get to the backup control centre? Do they have to travel from the main control centre, and if so, how long will that take and who will be in control of the railway while they are in transit? Alternatively, is the backup control centre adjacent to another control facility (another line, or another function) so staff with the correct qualifications are on hand? If so, how do they retain competence and familiarity with a different area of control, and potentially different technologies/processes? How are their duties in the other control facility covered?
- What main control centre loss scenarios are being considered? Is there equipment at the main control centre that if lost, would disable the backup control centre? Is the control system capable of an "uncooperative handover" of control of the railway infrastructure so that the backup control centre can take control even if the main control centre does not explicitly grant control (and if so, what safeguards are in place to prevent malicious use of this facility?)
- What level of service is required following loss of the main control centre? Is the objective of the backup control centre to run a completely normal service, to run a degraded, but still useful service, or simply to ensure that the railway can be safely evacuated and left in a state that will minimise further loss? Note that if the main control centre is along the line of route and has suffered such extensive damage that it is unavailable, it is likely that other elements of the line of route will also have suffered damage and so running a normal service will be unlikely.

The last question can be refined with an understanding of the time to restore the main control centre. The immediate requirement in the event of loss of a control facility is, as a minimum, to keep customers and staff safe, and minimising service impact is a nice-to-have. Once this has been achieved, the longer-term requirement can be considered.

- For some railways, the flexibility of network-based technologies and simplicity of service might mean that it would be possible to obtain some off-the-shelf computers, configure them with backups of control applications and data, and rig (and test!) a functional temporary control room in a suitable room in a day. In this case, the backup control facility can be simpler and focus on safe evacuation of the railway – although a clear plan for constructing a temporary control facility should be prepared, and operations and maintenance staff should regularly practice this plan.
- For other railways, particularly those with older control systems technologies, the control centre is a hive of specialist systems (with supplier lead times measured in months) with bespoke wiring which will require painstaking reconstruction, and the ability to create a temporary location limited by the dedicated point-to-point control cabling fanning out across the railway from a single geographical location. In this case, the timescale for restoration of the main control centre is likely to be measured in months, and the backup control centre will need to support a near-normal service for this period of time.

There are scenarios when a backup control room by itself can be of use; the majority of evacuations from main control rooms are due to environmental issues (e.g. premises defect, fire in nearby premises) and phased movement of control to a backup facility can be planned and achieved. A backup control facility also greatly facilitates routine maintenance (of all assets, not just train control systems) on a planned basis. However, railway operators should understand the limitations of their facility when planning for resilience.

4.2 Examples of how resilience can be achieved.

4.2.1 A mobile backup control facility

One railway has an excellent solution to how to maintain control of their infrastructure during a control centre evacuation; their backup control facility has been constructed in the trailer of an articulated lorry, which is parked at the bottom of the fire escape from the main control centre. The control systems are all IP-based, so a satellite link on the roof of the trailer can keep the backup control facility connected to the railway systems while in transit. In the event of control centre evacuation, the first operator can be in the trailer and regain simplified control of the railway before the last operator has left the control centre, and they can maintain sufficient control of the railway to co-ordinate evacuation while the lorry is being driven to safety.

4.2.2 A decentralised backup control facility

Building on this, we developed a novel resilience solution for a client who had experienced a painful total control centre failure on a fully automated railway. We had already identified that they would benefit from an application that would match available staff with trains stranded on the guideway in the event of a failure of the train control system; this system would:

- be hosted in the cloud so that it would be unaffected by loss of the control centre
- be accessed via a secure browser from any location so that it was not dependent on being in the control centre
- receive constant train position updates from the primary train control system
- receive constant updates on staff positions via a app on staff smartphones using GPS and Bluetooth beacons
- be able to rapidly identify the optimum plan for walking competent staff out to the last recorded position of stranded trains in the shortest time, validate this plan with the controller, transmit the plan in text form to staff smartphones, and continue to monitor staff movement to ensure that the plan was being correctly implemented.

This solution could do in seconds what would have previously taken the service control staff 20-30 minutes to do manually and produce a plan that would be faster to implement than one devised by a human. Not only would this get trains staffed (and hence moved to platforms) more quickly, but it would free up the service control staff do deal with the more strategic issues of the failure.

We built on this concept by:

- Proposing the routine control and monitoring of this system was on a tablet computer in a dock integrated into the control room; this provides power, communications and physical integration. This enables the tablet to be grabbed from the dock during a control room evaluation and so retained by the service controller who was running the railway immediately prior to the evacuation. The built-in battery and ability to communicate over wifi and cellphone services ensures ongoing connectivity with the cloud even if the control centre becomes unavailable.
- Adding other essential service control functions to the system, including staff messaging, VOIP communications, SCADA status and access to CCTV. This allows basic co-ordination of the railway to continue via the tablet following a control room evacuation. Human factors will dictate the limit of what can be achieved on a single tablet, but the system would support multiple tablets (e.g. one taken by each member of the control staff) which would then be used together.
- Communications (wifi and cellphone service) around the control centre (for control staff) and around the network (for staff smartphones) would be surveyed for signal strength and reinforced (diverse backhaul

and UPS) to ensure availability during a major incident. This also brings benefits for passengers under normal operations.

This solution now allows sufficient portable control of the railway to co-ordinate a rapid emergency evacuation compared to the previous situation, and at the fraction of the cost of a backup control centre.

4.2.3 Situational awareness through social media

A particular problem for unexampled or unimagined events is that the systems in a control room (e.g. SCADA, CCTV) might not give a full indication of the nature of an incident. An example of this was that when the London Underground network was bombed on 7th July 2005, the first explosion was originally interpreted as a failure of a high-voltage cable (as the initial symptoms were a localised loss of power supplies, and a loud bang) and the second explosion was initially thought to be a derailment.

Although as railways around the world modernise, the level of CCTV coverage and the detail of SCADA monitoring are constantly increasing, this is offset by the increase of train and station automation leading to a decrease in staff observation. Control Centre staff on a fully automated system cannot call upon the train driver to describe an incident; they have to rely on communications and SCADA systems, which may also be failing. This lack of situational awareness can lead to incorrect assumptions about the nature of an incident and therefore sub-optimal decisions of how to recover the service or evacuate passengers, leading to extended delays and increased levels of risk.

Situational awareness is essential for controlling transport infrastructure; even if an incident does not affect your own infrastructure, it might drive unusual passenger demand (e.g. as an alternative route) or unusual passenger behaviour or change in nature to threaten railway infrastructure at a later stage. Many control rooms are equipped with a dedicated TV news screen, access to dedicated weather stations or access to information from adjacent infrastructures. Driverless systems benefit greatly from real-time display of remote condition monitoring data; if there is no longer a driver to report a “rough ride” (e.g. a developing track defect) an on-train measurement of noise or vibration is a substitute. However, there is a lag in information being reported on news outlets and RCM data needs interpretation to spot anomalies, so these systems are not a complete solution.

The age of social media and high proportion of passengers carrying smartphones has brought near-instant photos and comments from the site of anything out of the ordinary. The level of information on an incident available on social media is as great as the level of information available in the control room from dedicated communication systems, but from a very different perspective. While information from social media may be opinionated, incomplete and potentially deliberately misleading, if it is made available to control centre staff in a suitably filtered form it can provide context to information from conventional sources (see figure 7).

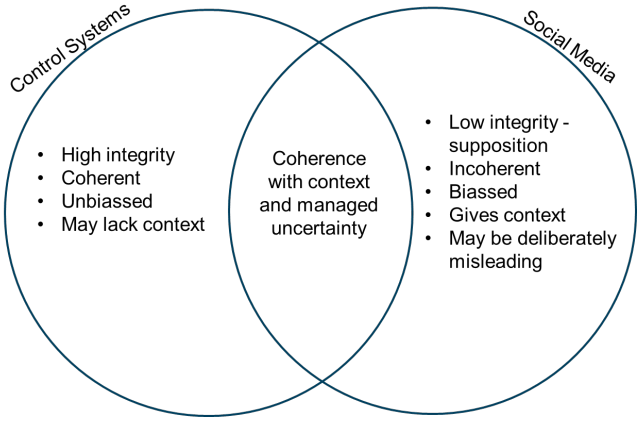

Figure 7: Situational Awareness from Social Media

Clearly this analysis needs to be pre-processed rather than expecting a service controller to surf social media all day; techniques like sentiment tracking can identify the initial stages of an incident, and AI filters can assist in sifting valuable information from the dross and presenting information that the service controller might wish to review. As well as using the combined eyes, ears and smartphones of the public to bring in pictures and comments to enhance situational awareness during degraded and emergency operating conditions, social media can also be used to

reassure and inform those trapped in trains if conventional communication systems have failed – if passengers feel that someone is in charge of an incident, they are significantly less likely to self-detrain.

4.2.4 Situational awareness through open data

Open data from other agencies often provides high-quality real-time data that can be used to give additional information to supplement control room systems. These include:

- Power supplies operators who have real-time feeds of reported power system disruption.
- Third party services that constantly monitor network infrastructure (these are generally faster to respond than the infrastructure supplier's dedicated status feeds!)
- Disruption information from other transport modes.
- Traffic flow information from roadside sensors – a wide variety of incidents lead to traffic disruption, whether roads are physically blocked or drivers are simply slowing down to take a look at an anomaly!

4.2.5 Commercial resilience

Modern technologies increasingly require support from the supplier to remain maintainable. Low probability high impact hazards can include failure/closure of a key supplier. This risk can be mitigated through:

- Obsolescence strategies, including stockpiling spare parts that would become difficult to source without the supplier, modularising the system with clear interfaces so that if a subsystem becomes unmaintainable, the smallest possible section of the system will need to be replaced.
- Escrow agreements, where any source code and know-how required to maintain a system are lodged with an escrow agent when the system is supplied and passed to the client only if the supplier ceases to be able to support the system. No intellectual property is lost be the supplier, but the client has an increased ability to maintain their system in the event of supplier failure.
- Avoiding proprietary technologies by using off-the-shelf hardware with clearly defined interfaces and ensuring that the source code, toolchain to build software and documentation is available to the client.

4.3 Practicing Resilience

Resilience plans will require staff to operate the railway in a very different way, and due to the nature of high-impact, low probability events, might only need to be invoked once in the career of even the most seasoned operator – if that often. It is therefore essential the familiarity with the processes is maintained through regular exercises using realistic scenarios, either played out on the desktop or using live action on the railway.

These exercises will bring additional benefits; by playing out different scenarios, the processes will be tested to identify shortcomings and opportunities for enhancement. By involving stakeholders outside the railway (e.g. government agencies, emergency service, local authorities, key suppliers, other transport authorities) in multi-disciplinary, multi-agency scenarios, the compatibility of the infrastructure processes and priorities of these different stakeholders will be tested, good practice can be shared, and relationships can be forged between the staff involved. These benefits will be of use when facing less extreme hazards that occur more frequently.

Scenario-based exercises are an excellent means of identifying issues such as:

- co-dependency, where the response of one group of participants assumes the availability of a service provided by another group of participants, unaware that this has also been impacted by the scenario. (e.g. the signalling incident manager attempts to call additional resources into work, but discovers that the phone system is inaccessible, or the mode of transport that staff would usually take is unavailable.)
- simultaneous call on common resources, where two or more groups of participants assume that they have the first call on a finite resource (e.g. vehicles, backup generators, blue light escorts) and discover that they have to wait for these resources to become available.

5 CONCLUSION

I would advise railway operators to:

- Ensure that their probability/impact curve is complete (including unnoticed/unmeasured as well as unexampled/unimaginable hazards) by not discarding potential hazards until they have been evaluated
- Look at advice from government agencies and the experience of other railways when identifying low-probability high-impact hazards
- Plan for failure scenarios rather than asset failures, using whole-railway thinking to find cost-effective techniques for maximising railway resilience
- Ensure there are diverse sources of situational awareness for service controllers, including non-conventional sources such as open data and social media
- Test their resilience before circumstances test it for you.

It is never possible to identify and mitigate all of the unexampled, unimagined events, but by identifying and mitigating the most obvious events, and ensuring there is sufficient organisational flexibility (and resilient communication) to allow a plan to be tailored to an unfolding scenario, the probability of successfully mitigating events (and reducing the impact on passengers, staff, infrastructure, and service) can be significantly increased.

6 REFERENCES

1. Westrum R. *A Typology of Resilience Situations* 2006
2. Lundberg J. and Johansson B. *Pragmatic Resilience [Online]* https://www.ep.liu.se/ecp/023/006/ecp2307006.pdf [Accessed May 2019]
3. Gaitanidou E., Tsami M. and Bekiari E. *A review of resilience management application tools in the transport sector [Online]* https://www.sciencedirect.com/science/article/pii/S2352146517303964 [Accessed May 2019]
4. Hollnagel E. *From regular threats to unexampled events: Risk, vulnerability, and complex systems* https://www.sintef.no/globalassets/project/samrisk/decris/meetings/hollnagel_decris_slides.pdf [Accessed May 2019]
5. UK Cabinet Office, *National Risk Register of Civil Emergencies 2017 [Online]* https://www.gov.uk/government/collections/national-risk-register-of-civil-emergencies [Accessed May 2019]
6. UK Cabinet Office, *National Business Resilience Planning Assumptions 2015 [Online]* https://www.gov.uk/government/publications/business-resilience-planning-assumptions [Accessed May 2019]