IRSE
Institution of Railway Signal Engineers

The ITC view on the residual risks to the Railway as at Q2 2018

Prepared on behalf of the International Technical Committee by Rod Muttram

Safe operation of the railway is a complex task, with many sources of risk. Command and control is just one area that needs to be considered in depth.
Photo Shutterstock/DaveNavarro Jr.

Imagine that you are being asked to endorse a new project or to reduce the scope of a running project due to budgetary constraints or time deadlines.

In the voluminous documentation presented, how do you identify and ensure suitable control and/or mitigation of those issues that may well affect safe operation of the railway?

We suggest that there are some key areas where you could certainly start:

- How will the way in which the railway is operated change?
- How do the changes impact on the technical and operational interfaces both from a permanent and a transitional perspective?
- How do the humans in the system, most importantly drivers and signallers/dispatchers, understand and deal with the changes, particularly transitions and operation in degraded modes during partial failure?
- Is there a reliance on long standing standards and practices, and if so are they still robust in the changed circumstances?

During the presentation day of the IRSE Annual Convention in Dallas on 26 September 2017, the IRSE International Technical Committee (ITC) presented three linked papers which we consider to be amongst our most important outputs in recent times. For that reason we have decided to produce this article to summarise those papers in a form that is digestible to non-signalling specialists. People make far reaching decisions affecting safe railway operation, but may not fully appreciate the implications and risks associated with proposals (which might appear superficially minor in nature) to change operational practice and/or the technical systems of infrastructure and rolling stock.

The three related papers cover a proactive approach to speed control, the need to recognise the importance of considering human factors and the methodology now used in the EU for railway risk analysis and management. They are primarily related to the main line railway (heavy rail) but a number of the messages and principles they outline are applicable to metros and light rail systems as well.

All ITC members are very experienced professionals. These three papers were prepared respectively by our current chair, Frans Heijnen, a former IRSE president, technical director of the ERTMS EEIG (European Economic Interest Group) and former vice president technology at Invensys Rail; by Rod Muttram, who as director, safety and standards led Railtrack's input to three of the four public inquiries into the Southall and Ladbroke Grove collisions before setting up the RSSB and then holding a series of vice president roles at Bombardier, and by Libor Lochman, executive director of the Community of European Railway and Infrastructure Companies (CER) and former director of the Railway Research Institute (VUZ) of Prague.

All of us are passionate about safety and the need for rail to protect, maintain and where possible improve its position in land transport safety performance.

Over 1.25 million people are killed every year on the world's roads. In the time it is likely to have taken you to read to this point, on average, 3 people will have died in road accidents. Despite these appalling statistics (or perhaps because the events are so frequent and common) road accidents get little publicity outside the areas where they occur. By contrast, rail accidents leading to fatalities become worldwide news. Consider the coverage of the Santiago de Compostela derailment in Spain in July 2013, the Bad Aibling collision in Germany in February 2016 and the derailment of an inaugural Amtrak service near Tacoma, Washington State, USA in December 2017. It is these types of infrequent but high consequence high speed derailments and collisions which the industry must continue to strive to eliminate.

We stress this because nothing is constant but change, and after a recent period of renaissance and significant growth the rail industry now potentially faces a new challenge from autonomous road transportation which allows the road sector to erode some of rail's competitive strengths. In the area of safety, the replacement of human drivers by autonomous driving systems offers the opportunity for the road sector to make huge improvements in safety performance and this will undoubtedly be something that the proponents of these technologies will emphasise.

The recent publicity around accidents involving Tesla cars believed to be driving using 'autopilot' (not a fully autonomous system) and Uber's (now suspended) self-driving trial in Arizona, would seem to indicate that the degree to which the public and media will accept a big incremental improvement in overall safety but with a remaining smaller residual risk of system error, is still unclear. No-one should underestimate the selling power of these global mega-corporations.

Rail must not be complacent: its average performance is very good, but it must be vigilant in maintaining that performance and continuing to improve in the areas that lead to the rare, but significant, major accidents and incidents. The three papers all drew heavily on the lessons from some of the recent more damaging ones and pointed to the sort of actions that will continue to reduce the frequency of such events.

Summaries of the papers

Paper 1: Adopting a proactive approach to the implementation of Speed Control Systems (Frans Heijnen assisted by Alan Rumsey)

The full paper can be found at irse.info/itc43.

Guided transport systems, and heavy rail in particular, have some characteristics that make them fundamentally different from road transport. Steel wheel on steel rail is a low friction system that gives low energy consumption but also leads to long braking distances meaning that drivers must often take action long before a curve that requires a reduced speed is visible to them.

At that point (for instance) they may be more prone to loss of concentration or distraction because they have had a low workload during a long period at constant speed and may not yet have recognised the approaching hazard. If they miss a lineside speed reduction warning, then by the time they do see the curve and perceive the risk it may be too late to achieve a sufficient speed reduction. This is one of the reasons why many driver training systems place such significance on 'route knowledge'. Further, if a train does enter a curve at higher than the safe speed then derailment, and quite likely overturning, is inevitable. There is nothing the driver can do to prevent or mitigate it, he/she cannot try to steer a different course in the way a road driver might if one is available.

The recent history of derailments due to overspeed highlights such deficiencies in the recognition of these risks associated with driver error. The behaviour of even the most vigilant and professional driver can be affected by external factors, such as pre-existing health conditions, shift patterns, distractions and the working environment. Changes to the track speed profile, whether permanent or temporary, customarily managed by use of signs, rules, and procedures are thus inherently prone to human error.

It is important to recognise that best practice is to have an operative engineered (automatic) control system like ETCS to underpin driver management of train speed. The emphasis is on 'operative' and it is vital to consider what happens when such systems fail, particularly at transitions between different systems or between areas where there is a system and where there is not.

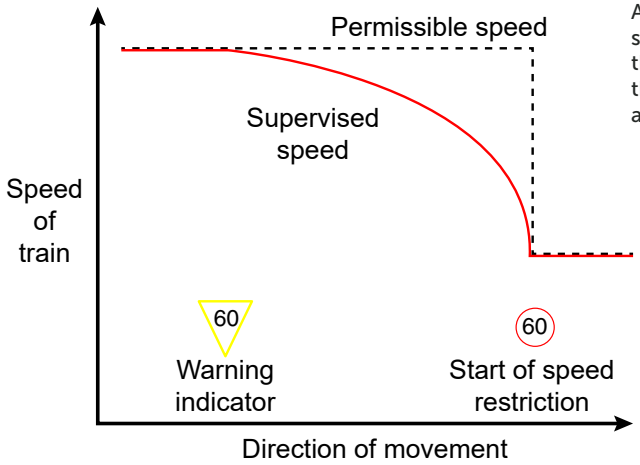
The paper makes the point that where a railway identifies such risks, or where action is forced upon them by Regulators, they have two choices; replace the existing signalling system with a newer generation of signalling technology that inherently provides the required level of safety protection; or overlay an additional system or systems on to the existing signalling system, to provide the additional safety protection required.

The paper describes a number of the systems of varying maturity that are available to fulfil the speed control function. Some are intermittent (fitted only where there is determined to be a high risk), while others provide continuous speed supervision. They have different whole life costs, operation, maintenance and training requirements and some may present much more of a challenge in terms implementation and transition from existing systems than others. Selection of the right system is therefore a complex issue but that does not justify doing nothing or excessive delay in taking action.

Risk assessments must thus cover more than just errors that relate to human interaction with the technology. It is often considered that long standing practices 'must be good enough' and they are not always challenged in the light of incremental changes happening around them.

At Santiago de Compostela the interface between new and 'traditional' infrastructure was a contributing factor, along with distraction and the use of a cruise control (speed hold) without the protection of an automatic braking system to prevent overspeed. The ETCS on-board the train concerned was switched off because of availability/compatibility issues and the track in the area of the accident was not yet fitted with the system anyway. The ITC believe that had the EU Common Safety Method (CSM) processes been followed in full to assess the system level risks, at least some of these issues would have been identified.

The paper concludes by making the observation that speed control is nowadays considered a 'must have' even if the business case is not always totally clear. The only thing sometimes missing is the recognition by all parties that times have changed. Automatic speed control is now a de facto norm and the assumption that the manual systems of the past provide sufficient protection is simply not defensible.



A continuous speed control system such as ETCS knows the maximum braking rate of the train and supervises the approach to speed restrictions.

Paper 2: How do we reduce the number of accidents due to Human Factors (Rod Muttram)

The full paper can be found at irse.info/itc47.

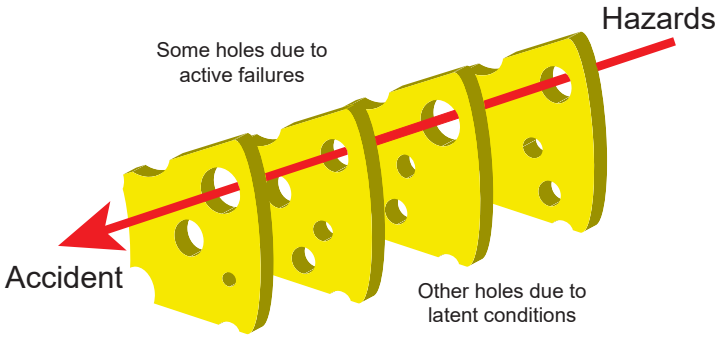
The performance of all systems is dependent on people, processes, equipment/tools and the interaction between them. Speed Control as considered in the first paper is one very representative example.

Human factors is a broad term for the analysis, understanding and optimisation of human performance in the work place. It should consider the working environment, interfaces and processes from a human-centred viewpoint, by looking at the whole system and its influence on the way people make decisions and interact with the other system elements and each other. Another (more or less interchangeable) term for this is 'Ergonomics' which has three branches:

- Cognitive ergonomics (concerning people's perception, reasoning, memory, motor response etc.).
- Organisational ergonomics (the impact of organisation structure, policies, processes, culture, etc.).
- Physical ergonomics (how people interact with equipment and tools including things like work layout, the design of symbology, required reach, strength etc.).

These three branches help us to understand why humans sometimes fail to do what they know only too well that they should.

Most accidents result from a combination of events, and human factors almost always play some part. The paper seeks to explain and illustrate this by presenting a number of industrial and railway examples and by using Professor James Reason's 'Swiss Cheese Model'. This represents safety barriers by slices of swiss cheese with holes randomly distributed in each slice representing flaws or weaknesses in those barriers. In a stable situation the holes in all the slices do not align in a way that lets something pass right through all the layers; but if there is 'noise in the system' that causes the layers to move, or something changes to introduce a new hole, a path can appear through all the barriers and that is when failures and accidents occur. Human factors often contribute those change factors.



Reason's 'Swiss Cheese' model recognises that multiple protections are necessary to ensure safety.

Risk assessment should seek to identify the potential weaknesses (holes) and aim to eliminate or mitigate them. For any system with people involved (and that includes the design of automated systems) an understanding of what makes people more prone to making errors is essential. Human performance is not a given – systems need to provide layered protection, and risk assessments should be cautious in assuming that different issues cannot occur simultaneously.

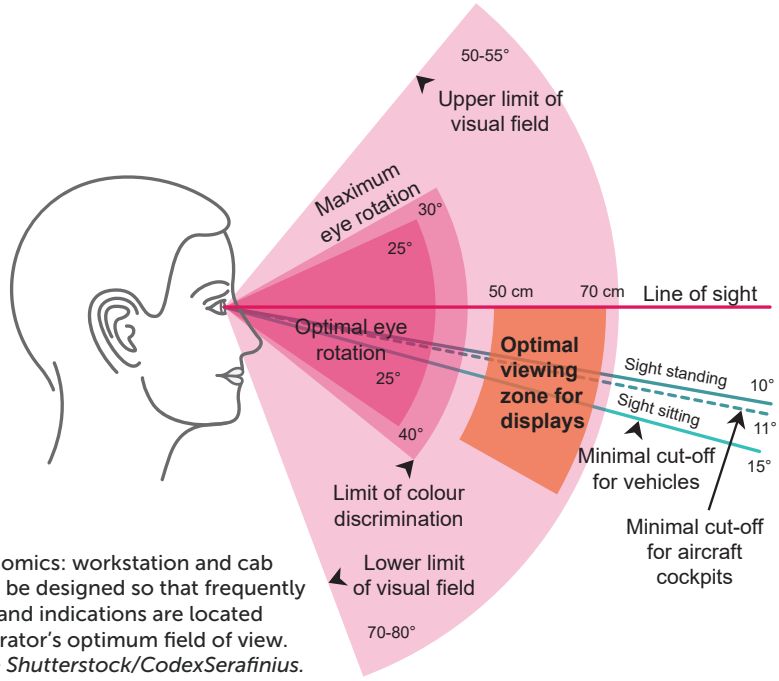
It is important to recognise that risk is not always a linear factor, e.g. increasing train density may cause a 'cliff edge' to be reached where risk suddenly increases markedly. Running in degraded (partial failure modes) where safety is more dependent on manual procedures always presents greater risk and needs to be planned for, and training provided. As one of the examples (Bad Aibling) illustrates, (and it is by no means unique), it is also possible for people to wrongly believe that technical systems have failed, even though they have not. Assessments should look for new emergent issues as well as incremental changes which can add up to significantly changed risk levels.

Safety systems should always include provision for the collection of data relating to human error both in normal and degraded modes in order to identify and then act to control or mitigate the factors that make errors more likely or even inevitable.

All railway businesses should have access to human factors expertise, and human factors must be integrated into all railway processes, particularly those involving significant change.

The increase in the use of automated systems of operation which are still designed by humans means that diligence is needed in design processes and system verification and validation (V&V) to reduce error rates. Early investment in a good system architecture, automated validation processes, the avoidance of over specification (and thus unnecessary complexity), and good system documentation for future maintainers will all pay later dividends. Once again planning for degraded modes of operation is essential.

The full paper sets out a number of other good practice pointers for human factors management.



Physical ergonomics: workstation and cab layouts should be designed so that frequently used controls and indications are located within the operator's optimum field of view. *Original image Shutterstock/CodexSerafinius.*

Paper 3: Improving the management of emerging and residual risks of Railway Control Command & Signalling (CCS) systems (Libor Lochman assisted by Jean Baptiste Simonnet – presented in Dallas by Francis How).

The full paper can be found at irse.info/itc48.

One of the aims of the European Union is to create a Single European Railway Area, supported by advanced regulations and standards delivering interoperability and a sufficient level of safety. There are emerging as well as residual risks in CCS technology and there is believed to be an insufficient knowledge of how to mitigate them (including the very topical risk of cyber security) without threatening system level safety, and decreasing system performance in terms of capacity and punctuality, and increasing overall cost. The EU believes that a harmonisation of safety practices can lead to better performance, reduced cost and therefore greater competitiveness for the railway sector. Whether you agree with that philosophy or not, the framework now produced does reflect acknowledged good practice in Safety Management.

Through the Railway Safety Directive the EU has introduced the Common Safety Method (CSM) for risk evaluation and assessment which for EU member states is a mandatory generic harmonised risk model. The rationale is that current practice should change and evolve towards a more harmonised approach that will contribute to improved rail performance. Harmonisation should help to reduce diversity and the impact of technical failures in a cost-effective way.

Within the European safety management framework, the CSM provides a detailed methodology for assessing safety risks related to any change within the railway system; it should also allow the identification and mitigation of degraded modes that can lead to severe consequences. It provides a guidance for safety hazard identification, analysing the risk impact from those hazards, defining relevant and suitable safety requirements and measures for accepting/managing residual risk.

Risk assessments may need to be adjusted to take account of hazardous cargos being transported by rail. *Photo Shutterstock/s_oleg*.

When the CSM is used properly the documentation trail produced can be an important tool for recording the 'corporate memory' of residual risk. CSM requires Railway Undertakings (RU) and Infrastructure Managers (IM) to have a collaborative Safety Management System in place and to use it to manage change.

Using CCS as an example, and the CSM Risk Assessment process, if the conclusion is that the risk does not need further reduction due to the system being compliant with established practices and standards, the associated decision must be justified and documented. This will also include explicit safety design targets.

There must be assurance that the acceptance criteria (code of practice, reference systems or explicit design target) is relevant. All interfaces within and to areas outside the scope of the change should also be very carefully considered.

CCS is only part of the overall railway system, and very often some risks are exported to other sub-systems or processes and to other duty holders e.g. where degraded modes of operation rely on operational rules and procedures. The risk handover process must not be unidirectional and the acceptance and understanding of these exported risks by those who have to manage them must always be negotiated and agreed and never assumed!

The paper concludes by saying that safety arguments based on long standing custom and practice, often embedded in rules and procedures, should be reviewed periodically, particularly when other changes are being made. Emergent threats like cyber attacks, incremental changes and increased usage over time can affect both rail and road traffic. A good example is the impact of these on safe level crossing operation; simpler crossing types may present an acceptable level of risk when rail and road traffic are light, but increase the traffic density, type or speed of either road or rail and more comprehensive risk control measures may be needed.

Conclusion

These three papers were intended as a call to action. Rail accidents with a significant loss of life or injury may be few and far between, but recent high-profile cases show that they are still headline news. With new competition emerging, the rail industry needs to be even better. The first two papers address the most common causes of recent significant accidents and the third sets out the rationale and opportunities for applying the structured methodology that the EU has developed. We commend them all to you and recommend that you take the time to read the full papers.

If you are a manager or responsible engineer in the rail industry then the ITC suggests that, to perform your role in a diligent manner, you should consider whether your safety management system is adequate. You should consider if it has been applied correctly and whether your organisation is using appropriate good practice solutions and engineered systems to protect staff from the errors they will occasionally make. Relying on past 'custom and practice' is simply not good enough.