International Engineering Safety Management

Paul Cheeseman

CEng MIET, FIRSE, MSaRS, London, UK

Dr Robert Davis

PhD, BSc (hons), FIET, FIMechE, FIRSE

Technical Programme Delivery Group

SUMMARY

This paper introduces the new international Engineering Safety Management (iESM) guidance for the worldwide railway industry that has been developed by Technical Programme Delivery Ltd (TPD) and reviewed by an international Working Group of senior practitioners, supported by MTR Corporation Hong Kong. The Group includes members from operating railways, regulators, manufacturers and subject experts from three continents. A new website www.intesm.org makes the guidance freely available and lists those who have been trained.

Following a period of consultation with a number of interested railways, suppliers and consultants, work was performed to complete the first international Handbook on Engineering Safety Management during 2012 such that it was no longer biased towards any particular legal system or regulatory framework for the acceptance of risk. It was launched in Hong Kong and Florida in April 2013, receiving enthusiastic support from those present.

INTRODUCTION

Formal system safety management has developed significantly during the last 20 years and whilst it has made a major contribution to preventing accidents during a period that railway systems themselves have become more complex and railways have become more intensively used. There have been a number of problems. Poor practice has seen

- the production of paper mountains instead of concise information and
- safety engineering starting too late after key decisions have been made resulting in safety work and safety cases being blamed for project delays and overspends.

Since 2000 significant development has continued within Europe on CENELEC Standards and guidance. Since YB4 was issued the Common Safety Method[1] has been established in European legislation, EN50128[2] was re-issued in 2011 and guidance notes supporting EN50129 on Cross Acceptance[3] and Assurance[4] have been issued.

In parallel, experience in the application of engineering safety management has matured throughout the world and many emerging economies needed guidance in moving their safety management towards good practice. Expertise is no longer UK –centric.

The main purpose of the Introduction is to enable the paper to be understood without undue reference to other sources. It should therefore have sufficient background material for this purpose. Generally specialized papers will not need extensive introduction as interested readers may be expected to be familiar with current literature on the subject. On the other hand, when a paper is likely to interest safety professionals working in fields outside the immediate area of the paper, the introduction should contain background material which could otherwise be scattered throughout the literature.

[1] Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety V1.1 2009

[2] Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems 2011

[3] Railway applications — Communication, signalling and processing systems — Application Guide for EN 50129 Part 1: Cross-acceptance PD CLC/TR50506-1:2007

[4] Railway applications — Communication, signalling and processing systems — Application guide for EN 50129 Part 2: Safety assurance PD CLC/TR 50506-2:2009

iESM WORKING GROUP

The aim of the iESM Working Group (iESM WG) is to assist the international railway industry in delivering acceptable levels of safety by promulgating good practice in railway Engineering Safety Management. The iESM WG pursues its aims by:

- Acting as Design Authority for iESM for Engineering Safety Management guidance and any associated supporting materials (e.g. Application Notes, templates and checklists);
- Facilitating the efficient and effective application of iESM for Engineering Safety Management;
- Promoting and facilitating the exchange of ideas for good practice that are found in the world railway community and other relevant industries; and,
- Setting up and overseeing support groups as necessary.

The scope of activities excludes certification of people, products or services. iESM WG activities are performed on a not-for-profit basis by practitioners supported by their employing organisations.

The iESM WG proceeds by consensus which may sound like a recipe for inaction. In practice the desire to make progress has outweighed any political posturing or technical esotericism. The initial Chair is Dr Robert Davis (a former chair of the original Yellow Book Steering Group) and meetings have been held approximately quarterly so far in Hong Kong, London and Vancouver. RSSB in UK is supporting this initiative with a view to sharing GB rail experience and practice in the safe management of engineering change and also to identify good practice from these other companies, some of whom are working on extremely ambitious rail programmes.

iESM WG membership aims to be broadly representative of the international railway community. All members of the iESM WG are:

- Recognised as having significant standing within the industry on matters relating to the management of safety,
- Available and committed to the work of the iESM WG; and,
- Able to provide a professional contribution to iESM WG activities based on their skills and expertise.

iESM PRINCIPLES

iESM has been written principally for people around the world who use their judgment to take or review decisions that affect railway safety and to help them exercise their judgment in a systematic and informed manner. The iESM Principles, processes and flows of information between them are shown in Figure 1 below. The activities in the darker boxes represent the main flow of the ESM process while the activities in the lighter boxes represent supporting activities that are performed throughout the durations of the activities in the darker boxes. The Principles are arranged under five headings:

- Definition
- Risk analysis
- Risk control
- Technical support
- Team support

It is important to emphasise that iESM is not an “add-on” overhead – it should be an integral part of all engineering activities. It may be that your organization draws the boundaries between activities in different places or gives them different names. How they are structured and named makes no difference to their effectiveness. What matters is that they should be done, and done well. iESM provides a structured and systematic approach to managing railway system safety and aims to provide good practice – all in one place.

This paper has space only to show some of the highlights of iESM. In summary, the new iESM guidance:

- Is advisory, not mandatory.
- Fills a gap left by the former UK ESM guidance known as “Yellow Book” which was used extensively around the world, not just in English speaking countries.
- Supports use of CENELEC standards and Common Safety Methods (CSM) for risk assessment, with practical, cost-effective advice.
- Should assist in discharging legal & professional obligations.
- Is guided by an international Working Group of practitioners and supporters giving it credibility with the avoidance of bias.

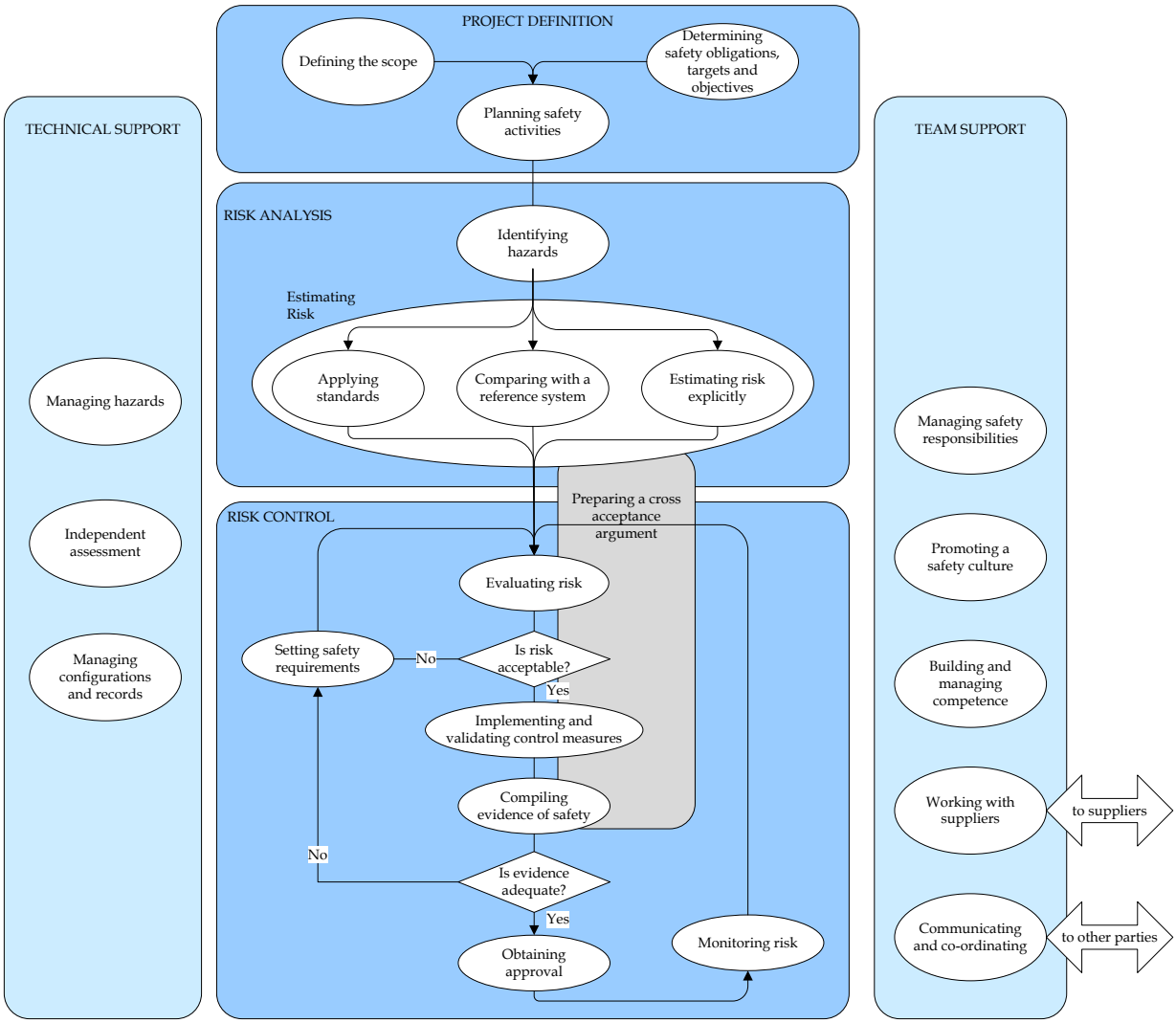

Figure 1: iESM Principles and Processes

USING THE iESM GUIDANCE

iESM is not an "add-on" overhead – it should be an integral part of all engineering activities. You may find that your organization draws the boundaries between activities in different places or gives them different names. The generic ESM process contains activities, such as configuration management, which are essential to deliver safety but are also required for other reasons. There may be activities in the generic process that your organization chooses to regard as parts of other processes. How you structure and name these activities makes no difference to their effectiveness. All that matters is that they should be done and done well. iESM provides a structured and systematic approach to managing railway system safety.

The guidance does not provide a complete framework for making decisions about railway work. It is concerned with safety and does not consider non-safety benefits. Even as regards safety, the guidance does not dictate the values which underlie decisions to accept or reject risk. However, it does provide a rational framework for making sure that such decisions stay within the law and reflect the organization's values and those of society at large and then for demonstrating that this is the case.

Some railway companies have chosen to build the iESM guidance into their own Safety Management Systems. They have linked it to their competency arrangements as a way of objectively demonstrating that their staff are trained and capable of doing the work required of them. Training and certification is available on behalf of the iESM WG to suit most needs:

- Conversion or refreshing from other engineering safety management training with exam
- One day Practitioner course with exam
- Optional second day Practitioner with a practical case study
- Hazard identification and management
- Independent Safety Assessment

All those trained are listed on www.intesm.org. Suppliers too have found it useful when working in an international market so that they can reuse safety evidence more easily.

SUMMARY OF iESM GUIDANCE

Within this paper it is only possible to give an outline of the guidance. At its core are three main approaches to risk management – compliance with standards, comparison with a reference system and explicit risk estimation. These are the three parallel paths in Figure 1. Importantly these three approaches are integrated into one framework, to make most effective use of time and resources. Typically Civil Engineers rely on standards to manage risk, whilst those developing more novel signalling systems might adopt a quantified risk assessment approach and at other times simply repeat what was done at another location. iESM allows for all these approaches. It also overcomes some of the criticism of previous guidance which was seen to be too onerous for low risk projects whilst at the same time providing little help to those for who standards compliance is inadequate in specific applications. The approaches are illustrated in the following subsections. Note they are applied to hazards not at (sub)system nor project level. The importance of robust and vigorous hazard identification remains.

Compliance with Standards

If a hazard is fully addressed by accepted standards (or Codes of Practice as the CSM [2] calls them) that define agreed ways of controlling it, showing that you have complied with these standards may be enough to control the hazard or to meet your legal obligations (or both). For example, the electrical safety of ordinary office equipment is normally shown by meeting electrical standards. iESM uses the word 'standard' to include other forms of authoritative guidance such as rules and codes of practice.

Any standard shall at least satisfy following requirements:

- Be widely acknowledged in railway domain. If not the case, the standard will have to be justified;
- Be relevant for control of considered hazards in system under assessment;
- Be publicly available for all who want to use it.

However as the Hazards Forum [6] reminds us "Mere compliance to standards is unlikely to be regarded as evidence that sufficient care has been taken or that best practice was followed. It will be necessary to demonstrate that the standards complied with are relevant and appropriate to the system and the circumstances in which it was to operate." This must therefore form part of our safety argument. Compliance with standards can be (almost) sufficient if all of these are true:

- The equipment or process is being used as intended
- All the risk is covered by the standard(s)
- The standard(s) cover your situation
- Users of the standard have sufficient understanding of current good practice and the world around them
- There are no obvious or reasonably practicable ways of reducing risk further

An example of this approach is providing lighting on platforms that complies to current standards during an upgrade. However at the station situated just beyond a long tunnel section the modern lighting may be so bright and dazzle the driver. Risk monitoring (an iESM Principle) is valuable to monitor the situation to see if other measures need to be taken.

However, this approach has limits and other approaches as described below may be necessary.

Reference System

If you can show that your system is sufficiently similar to a reference system - another system that is known to be safe, and that the risk associated with some hazards of your system is no more than that associated with the reference system, then you may be able to conclude that those hazards are controlled. This can be effective but requires a suitable similar system - and significant amounts of information about it - to form the reference. This is not always available.

This approach has been used in some countries extensively and is similar in concept to the Globalement Au Moins Bon (GAMAB) as described in CENELEC EN50126 but applied at the hazard level rather than the system level.

A Reference System shall at least satisfy following:

- It has already been proven in-use to have an acceptable safety level and would still qualify for acceptance where change is to be introduced;
- It has similar functions and interfaces as system under assessment;
- It is used under similar operational conditions as system under assessment;

- It is used under similar environmental conditions as system under assessment.

Note also that this is not a “cross acceptance” process as described in the CENELEC standards but simply a comparison at the level of a hazard. An example might be stepping distances on an older railway where the cost to eliminate platform gaps would be high and the most effective risk control would be to close the station – clearly an unacceptable outcome. However on a network where passengers are used to the step and other mitigation measures are in place (for example illumination, painted warnings and announcements) this hazard may be managed through reference to a similar station having comparable distances, trains and passenger loadings).

Explicit Risk Estimation

This approach will be familiar to those who used “Yellow Book” and most other Quantified Risk Assessment approaches. You may make an explicit estimation of the risk, that is, you may estimate the frequency with which incidents will occur and the harm done, either as numbers or by selecting from a number of categories. It is useful and can be accurate but it is time consuming and requires significant expertise. It is however, the only way to deal with new risks or very significant risks.

The need for explicit risk estimation could arise:

- When the system under assessment is entirely new and therefore there is some uncertainty, OR
- Where there are deviations from a standard or a Reference System, OR
- When the chosen design strategy does not allow the usage of standard or similar Reference System because for example, of a wish to produce a more cost effective design that has not been tried before.

One major contribution of this approach is that explicit risk estimation allows modelling of the interactions between the various risks in order to show the combined effects and, if required (it normally is!), the overall risk level. It has also been said that doing the thinking to produce a QRA model is almost as important as the result of the model itself. In this paper we will not repeat the methods described extensively elsewhere.

Novelty and complexity can be thought of as measures of the uncertainty of outcome – the likelihood that the proposed change, once implemented, will or will not behave as predicted. The more novel and the more complex a change or a technology is, the higher the likelihood that it may behave in an unpredicted and possibly undesirable way. Therefore, the more novel and the more complex a change is, the more it is likely to need an explicit risk estimation approach. It is necessary to consider both what is innovative in the railway industry, and what is merely new just for the organisation implementing the change.

Technical Support

Not only is it important to produce safe work, it is necessary to demonstrate that you have produced safe work. This group contains three activities that provide technical support to the other iESM activities and help provide evidence for the safety argument. They are “cross functional” in that they require contribution and commitment across the organizations performing the work. These three important supporting acts to iESM are:

- Hazard identification
- Independent Assessment
- Configuration Management

The challenge is that these activities cross functional boundaries and are typically performed differently by different departments / functions.

Team Support

This group contains a number of activities that support the iESM activities discussed so far by ensuring that the people involved in these activities are competent and well-organized. Some, could be called structured common sense so won’t spend a lot of time explaining them here.

One however, is unique to iESM and has been shown by experience to be very, very important - “Promoting a safety culture”. This underpins most of the iESM activities and requires sustained commitment. The Principles here are:

- Managing safety responsibilities
- Promoting a safety culture
- Building & managing competence
- Working with suppliers
- Communicating and co-ordinating

CONCLUSION

Absolute safety is not achievable in the real world and therefore success relies on two fundamentals:

- good processes, and
- good people;

such that when there is a problem or failure in one, the railway can be sustained by the other.

If you already have an ESM process in place, we hope that you will use the generic iESM process described here as a benchmark for assessing your process. If you do not already have an ESM process, we hope that you will find the generic process useful for creating one. For every activity, you will be able to find guidance in volume 2 of the iESM handbook on performing that activity. You do not have to use the approach described and it is not the only effective approach, however it has been proven in practice and has the support of some of the leading professionals in the world.

The intention is that iESM provides good practice guidance and will continue to reflect emerging good practice. iESM doesn't claim that it is always best practice and does not stop you going further or doing more. Finally, iESM resources and a list of competent practitioners may be found at www.intesm.org.

ACKNOWLEDGEMENTS

The significant support of the Directors of Technical Programme Delivery Ltd in the development of iESM is acknowledged as is the support for the iESM Working Group by MTR Corporation Hong Kong. The members of the iESM WG are thanked for giving their time and expertise freely and effectively towards the usefulness and accuracy of the resulting guidance.