

international Engineering Safety Management – Assessment Accreditation Scheme

P.Cheeseman¹

CEng MIET, FIRSE, MSaRS, London, UK

Overview

This paper introduces a scheme for independent safety assessment accreditation within railways, in line with the CENELEC suite of Railway Application standards, as part of the international Engineering Safety Management (iESM) guidance for the worldwide railway industry. The iESM Guidance was developed by the TPD Group and reviewed by an international Working Group of senior practitioners, supported by MTR Corporation Hong Kong. It was presented at IRSC in Vancouver in 2013. It is freely available from www.intesm.org and includes guidance on performing Independent Assessment.

iESM Accreditation – Why?

The role of the Independent Assessor is critical to assure satisfactory evidence of safety before operation or after modification. Whilst the iESM guidance and others have described the process of independent assessment and even listed the expected qualifications of an Assessor, this work was carried out to address a rather glaring gap in assurance of the engineering safety management lifecycle activities. Whilst there are various licensing schemes in rail (e.g. signaling-related activities), there has never been a recognized accreditation scheme for safety assessors.

Railtrack in UK, and for a time their successors Network Rail, operated an in-house scheme that provided accreditation to companies providing independent safety assessment services. Since then in Europe various mandatory accreditation schemes for Assessment Bodies (under the Common Safety Methods for Risk Assessment), Notified Bodies (under Interoperability Regulations) or Design Bodies (under National Notified Technical Rules) have been developed. Whilst similar, none of these covers the risk-based independent safety assessment role and all of them bring a significant overhead of accreditation assurance.

The emerging draft (at the time of writing) of CENELEC EN50126-2 includes a set of key competences for an Assessor including having an

“acceptance/license” from a recognized safety authority. The standard offers no further guidance on what is expected or how it may be achieved. The iESM Accreditation Scheme aims to meet this requirement.

Company or Individual?

Existing accreditation arrangements such as they are aim at accrediting organizations rather than individuals. Typically companies will have internal processes for ensuring that staff or contractors are competent for the work they are assigned to. In the Railtrack / Network Rail example a competency matrix was used to indicate one of 5 levels of ability against a long list of tools & techniques, roles and lifecycle activities. This is supported by a record of training (although as discussed below not any ISA-specific training) and education. Supporting processes require these to be kept up to date. There is no assessment of any such training nor any measure of the currency of any claimed experience.

That process was defined to meet the needs of one, albeit significant, large client. It is not easily transferable to the needs of another client and could lead to multiple versions of similar but different matrices existing. Nor, for the individual are they easily transportable to other companies.

Thus such corporate arrangements, whilst important, are limited in that they:

- do not necessarily meet the needs of particular projects (which is surely the core requirement);
- maybe single client focused;
- are rather subjective.

The European schemes for AsBo focus heavily on the processes (such as managing certificates) and organization of the company (such as management control). This requires substantial overhead and demonstration of compliance through audit. The effect has been that only larger companies can achieve and maintain these certifications whilst smaller niche providers are excluded. Further it turns independent assessment into a product line which means companies specialize in provided the service to the exclusion of providing safety engineering services on projects to demonstrate safety. Both these factors have an inadvertent emerging property of increasing cost without any demonstrable improvement in safety assurance.

Achieving the iESM mark will depend on the context and the environment in which the independent assessment is performed and also on the working culture of the organization. In a commercial environment the standard of competence is the standard of work expected to satisfy a number of requirements, including business objectives as well as the more obvious safety requirements.

Requirements for a scheme

The new iESM approach reflects that the delivery of effective safety assessment relies fundamentally on the skill, experience, competence and independence of individuals sometimes working as teams, supported by the processes of corporate entities, rather than the other way around. These requirements drawn for EN50126 and iESM are shown in the table below.

No	Requirement
1	Be competent in the domain/technologies where independent assessment is carried out
2	Have acceptance / license from a recognized safety authority
3	Have / strive to continually gain sufficient levels of experience in the safety principles and the application of the principles within the application domain
4	Be competent to check that a suitable method or combination of methods in a given context have been applied
5	Be competent in understanding the relevant safety, human resource, technical and quality management processes in fulfilling the requirements of the EN 50126
6	Be competent in independent assessment approaches/methodologies
7	Have analytical thinking ability and good observation skills
8	Be capable of combining different sources and types of evidence and synthesize an overall view about fitness for purpose or constraints and limitations on application
9	Have an understanding of the overall system including its application environment
10	Understand the requirements of EN 50126
11	Professional status in an engineering or scientific discipline relevant to the system or equipment
12	Prior experience as an independent assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment
13	A commitment to safety

No	Requirement
14	The flexibility to adapt to changing circumstances and the perform assessment tasks efficiently and to minimize wastage of physical and virtual resources

Where an independent assessment is carried out by a team, the team as a whole should possess the technical knowledge and experience and the Lead Assessor as an individual should possess the personal qualifications and attributes.

iESM Approach

The iESM approach offers a combination of some company processes and the expertise of individuals demonstrated largely by self-assessment and professional registration.

Companies can carry the iESM accreditation mark as a service provider but only if they deploy suitably qualified and experienced assessors. Assessors can achieve the iESM accreditation mark but only if operating within a minimum organizational framework (not necessarily their own company) and relevant professional registration . These marks can be achieved by meeting the requirements in EN50126-2 as expanded by the guidance in iESM where necessary.

For individuals there are three requirements which have been expanded into competencies by the Institution of Engineering and Technology and British Computer Society in their publication "Safety Competency and Commitment":

- Behavioural competence – including for example maintaining independence
- Technical competence e.g. safety engineering and risk acceptance techniques, assessment and audit, general consultancy skills
- Knowledge – legal requirements, domain, system, technology, specialist areas

Professional Registration

The iESM approach requires that a Lead Assessor be professionally recognized, for example Chartered Engineer or Professional Engineer status in Australia. The professional institutions have robust and established processes to recognize those with an appropriate standing within the industry. Membership includes a commitment to a Code of

Conduct which effectively covers the behavioral Independent Assessment issues relating for example to conflict of interest and objectivity. Other Assessors on a team do not need to be corporate members of institutions allowing for flexibility and professional development, however they will need to sign an identical Code of Conduct.

Technical Competence

To date approximately a thousand people have taken the iESM Practitioner's course and most have passed the exam at the end of it.

Their achievement is recorded on the iESM website (see www.intesm.org/training-approved-practitioners.html). A similar list of Independent Assessment practitioners is being developed following the pilot. Passing the iESM Practitioner's Course demonstrates an understanding of the iESM requirements – including, at a high level - independent assessment and the requirements of the CENELEC family of Railway application standards.

Once this has been undertaken and the exam passed, an iESM Independent Assessment course, developed around Application Note 4 on www.intesm.org develops the specific competences and gives classroom experience of performing assessment. The course is intensive and covers:

- The need for a Independent Assessment and how it can reduce project and safety risk;
- Key Independent Assessment concepts and terminology;
- Planning an Independent Assessment;
- Good practice tools and techniques for Independent Assessment and apply the AN4 guidance on implementing them, including:
 - Deliverable assessment
 - Observation categorization
 - Safety audit overview
 - Diverse analysis
 - Vertical Slice Analysis
 - Sampling
 - Managing outcomes

More detail is shown here

http://www.intesm.org/ISA_training_overview_01.pdf The exam is deliberately harder than that for iESM Practitioner. Success in the

course exam is good evidence for a number of the competencies identified below.

Self Assessment – three levels

There are four key competencies that apply to almost all projects:

- acquiring an appreciation of the scope and context of the assessment;
- selecting and planning a cost-effective assessment strategy;
- gathering relevant evidence;
- forming a judgement including managing any outcomes.

Many competency frameworks define levels using terminology which can be confusing and divisive. The iESM Scheme uses three numeric levels.

Level 1 is the base level which indicates that the Assessor has sufficient knowledge and understanding of good practice to be able to work on assessment tasks without placing an excessive burden on other consultants which might compromise safety or quality. Level One Assessors may not have had previous experience of working on rail industry projects. It may therefore be necessary to extrapolate from evidence of technical skills derived from a non-rail-related project environment. Their competencies are likely to have been developed through targeted training and work on non-assessment projects.

At Level 2, the Assessor has sufficient knowledge and understanding of good practice and has sufficiently demonstrable experience, to be able to work on the tasks associated with the overall activity without the need for detailed supervision. A Level Two Assessor will maintain their knowledge and be aware of the current developments in the context in which they work. . A Level Two Assessor may be required to perform detailed checks on the work carried out by a Level One Assessor.

At Level 3, the Assessor has sufficient understanding of why things are done in certain ways, and sufficiently demonstrable skills, to be able to undertake overall responsibility for leading a task or project. A Level Three Assessor will be familiar with the ways in which systems or products have failed in the past. They will keep abreast of technologies, architectures, application solutions, standards, and regulatory requirements. They will have sufficient breadth of experience, knowledge and understanding to be able to work in novel

situations. They are able to deal with a multiplicity of problems under pressure without jeopardising safety or quality issues.

There are six specific elements within the Independent Assessment competence (excluding audit) as shown in the table below linked to the three levels to aid self assessment. Note one key competence is auditing. This is not covered by the iESM scheme as there are many comprehensive auditing recognition schemes existing.

Title	Description	Typical Performance Level
Scope & Content Appreciation	Acquires an appreciation of the product or system and the application to which it is being put. Establishes the scope and objectives of an assessment, such that all necessary requirements of a safety assessment are capable of being satisfied.	<p>Level 1: Understands broadly the use and scope of the product or system in question within the wider railway.</p> <p>Level 2: Can describe the safety implications and functions of the system and product, and how these relate to the wider railway in providing acceptable levels of risk. Can use this understanding to identify key aspects of the product or system to be assessed.</p> <p>Level 3: Understands how the wider railway interacts with the product or system under question, and can see how changes to the system boundaries or in approach might affect the safety argument. Uses this deep system knowledge to formulate a strong understanding of the scope of the assessment.</p>

Title	Description	Typical Performance Level
Assessment Strategy Selection and Planning	Selects an assessment strategy involving a range of techniques and measures which are capable of yielding sufficient evidence in a cost-effective manner to enable a robust judgment to be made regarding the safety of a product or system. Encapsulates the assessment strategy in a workable plan.	<p>Level 1: Understands that an IA Plan contains a description of the review, audit, analysis and test witnessing work required to form a judgement on the safety of a product or system. Appreciates the need for different levels of rigour.</p> <p>Level 2: Shows understanding of the different assessment techniques and their strengths and weaknesses, including how they might be performed in practice. Has written several IA Plans, or similar types of plan for conventional systems and low/medium integrity systems.</p> <p>Level 3: Has reviewed and signed off ISA Plans. Can develop an assessment strategy for a novel and/or high integrity products or systems. Understands the difference between techniques and how some combination of techniques may not be effective in providing a proper assessment of key safety aspects of products or systems, and how other combinations may not be cost effective.</p>

Title	Description	Typical Performance Level
Reviewing Safety Documentation	Accurately and systematically reviews documents, supported by discussions to clarify ambiguities and understanding where necessary, to obtain evidence to support a judgment on whether a product or system has satisfied its functional safety requirements.	<p>Level 1: Able to perform reviews on safety cases, hazard procedures, safety plans, and produce a relevant set of observations.</p> <p>Level 2: Has performed reviews and produces relevant observations on quality of the information in the documents, and highlighting items that would normally be expected to be included. Can look outside the system boundary. Able to categorise observations in line with the classification system.</p> <p>Level 3: Has reviewed and signed off reports on reviews of safety documentation and can identify astute observations on safety documents including those which could have a significant impact on the overall safety argument for the product/system. Can recognise common issues and reflect that in the observations made. Is able to categorise observations so that the key issues to be addressed are highlighted and can determine when large numbers of lower category observations should be reflected by higher categorisations. Understands the problems with producing safety documentation based on issues faced when working on safety engineering projects and can apply this knowledge to assessments.</p>

Title	Description	Typical Performance Level
Assessing Safety Analysis	Determines the completeness of safety analyses. Identifies, where necessary, the requirements for further safety analysis to obtain evidence to support a judgment on whether a product or system has satisfied its functional safety objectives.	<p>Level 1: Is aware of the purpose of safety analysis, and what an ISA may wish to determine when performing an assessment on a safety analysis for a product or system. Understands the difference between Cause, Hazard, Accident and Consequence.</p> <p>Level 2: Appreciates the difference between HAZID and HAZAN studies, including detailed FMECA and FTA analyses. Has performed reviews on safety analyses and hazard logs and picked out relevant observations. Can identify confusions between Hazard, Cause and Consequence.</p> <p>Level 3: Has experience in performing safety analyses for a range of systems and products, and can identify holes in safety work in terms of providing a full argument that the system or product is safe. Aware of how the risk assessment process feeds into the final safety argument and can take a view on how the iESM processes can be tailored to meet a project's specific needs.</p>

Title	Description	Typical Performance Level
Producing assessment reports including formation of an overall judgment on the safety of a product or system, or process used.	Produces succinct and comprehensive reports on assessment work carried out containing an unambiguous judgment, through a reasoned and documented argument, on whether a product, system or process has satisfied its safety objectives.	<p>Level 1: Able to form a conclusion based on a list of findings, and write up a body of assessment or audit work to produce a good quality report.</p> <p>Level 2: Understands the relative importance of different findings from the assessment work carried out and can balance them to produce a considered judgement on the safety assurance of a system or product. Has produced several assessment reports.</p> <p>Level 3: Has helped in or produced the overall conclusions on an assessment project where many different people have had an input, and produced a balanced, well-written report. Is able to show how the report stood up to scrutiny and challenge from the project or a third party (e.g. regulator or approval body).</p>

Title	Description	Typical Performance Level
Managing Outcomes	Contributes as required to the management of the results of a safety assessment, such that any necessary actions are addressed and appropriately resolved.	<p>Level 1: able to agree closure of individual observations raised by themselves based on an acceptable project response.</p> <p>Level 2: has managed the resolution of observations raised by a set of assessors and able to reach compromises in areas where there is some dispute, without affecting the level of safety integrity.</p> <p>Level 3: Has experience of presenting assessment results to potentially hostile projects and acceptance bodies and is able to negotiate a way forward. Keeps the safety principles of the assessment to the fore when reaching agreements while being flexible in agreeing an appropriate way forward. Is firm in defending key assessment findings. Able to remain calm and controlled when under significant pressure.</p>

Domain Knowledge

The generic domain knowledge is dealt with in a similar way the Technical Competence described above using three levels:

- **Level 1:** The individual possesses a basic understanding of the Domain Element (at least 80% of the Element), including its scope, function and general principles of operation/application. Capable of placing the Element in the context of the wider railway and is aware of the critical/important interfaces. May not have worked on projects involving this Element before.
- **Level 2:** The individual possesses a detailed understanding of the Element, including key failure mechanisms and operation under degraded or abnormal conditions, having worked on one or more projects specific to, or inclusive of, the Element. They have had

direct experience of at least 80% of the topics within the Element; any exclusions and developing specialisms should be stated.

- **Level 3:** The individual possesses an authoritative understanding of the Element, having been involved in several phases of the system lifecycle, including development/design, manufacture, installation, operation/use and maintenance/modification, for at least 80% of the topics within the Element. Any exclusions and specialisms should be stated.

For each Element, the level of knowledge and experience is expected to reflect the understanding of the underlying principles, knowledge of relevant standards across various railway administrations (specifically noting specialisms and exclusions) and relevant experience of the product, system, equipment or process.

The '80% rule' described above is a broad 'rule of thumb'. It is *not* intended that consultants calculate the exact proportion of the topics within the Element that they understand. It *is* intended to be used pragmatically. For example, in the 'widget' Element, there may be twenty different types of widget, but only five are commonly used; therefore understanding of four of the five commonly used widgets would fulfill the 80% rule.

Whether a consultant can be considered to have attained a particular level is ultimately judged at the discretion of the Responsible Manager.

Demonstration of Competency

The role of the designated "Responsible Manager" is key within the organization. With an individual working alone this role may be performed by the iESM Secretariat. The Responsible Manager will make the judgment as to whether an individual is competent at the appropriate level, even if the individual has not actually performed the role before. This might be on the basis of what else they have done, what they have experienced, the efficacy of any training they may have received plus other relevant technical and behavioral abilities.

In the absence of past assessment experience, the Responsible Manager will seek other assurance through, for instance:

- a demonstration that the Assessor would be able to apply the competency correctly in a hypothetical situation (*can be applied*);
- the ability to answer questions pertaining to the competency based on past experience (*can be tested*);
- evidence of having been trained in that particular competency (*has been shown*).

The nature of the evidence to demonstrate competence needs to be considered. It is acknowledged that documentary workplace records are not always available and sometimes access to them may be inappropriate so the Responsible Manager can allow other forms of evidence at their discretion. Other forms of evidence that might be considered are:

- assignment and/or project records;
- documentary records;
- workplace observation;
- competence test (see below);
- witness testimony;
- oral testimony.

It is certainly not a requirement of the iESM scheme that copies should be made of evidence or separately filed, ready to be produced on demand. There needs to be adequate referencing to evidence, but except where there is some doubt or disagreement, it is not necessary to physically obtain the evidence itself.

Conclusion

This new iESM Accreditation scheme is available for individuals and independent assessment service providing companies. It has been piloted in Australia and should fill a gap in the assurance arrangements for clients and suppliers alike. It aims to be “light-touch” but give substantial credibility to the assessors who achieve the mark through a combination of training, experience and demonstrable competence.

Refinements will be made as experience grows and in response to emerging requirements from the international standards.