# international Engineering Safety Management

## Good Practice Guidance

## Application Note 4
## Independent Assessment

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd
Issue 01, Mar 2014

We are grateful to the organizations listed who have supported iESM in various ways:

Cover pictures © 2012 Paul Cheeseman

## Disclaimer

Technical Programme Delivery Limited (TPD) and the other organizations and individuals involved in preparing this handbook have taken trouble to make sure that the handbook is accurate and useful, but it is only a guide. We do not give any form of guarantee that following the guidance in this handbook will be enough to ensure safety. We will not be liable to pay compensation to anyone who uses this handbook.

## Acknowledgements

This Application Note has been written with help from the people listed below.

- D Beacham
- Dr G Bearfield
- S Bickley
- N Bowley
- M Castles
- P Cheeseman
- Dr Chen Roger Lei
- J-M Cloarec
- Dr R Davis
- B Elliott
- T Jones
- Dr KM Leung
- Ms J Myde
- Ng Nelson Wai Hung
- G Parris
- Sen Paul HB
- Mrs Shi Lisa
- A Russo
- G Topham
- Dr Fei Yan
- Dr Zhang Simon

These people worked for the organizations listed below.

- Abbot Risk Consulting
- Arbutus Technical Consulting
- Beijing National Railway Research and Design Institute of Signal and Communication Co. Ltd.
- Beijing Traffic Control Technology Company
- Bombardier Transportation
- Certifer
- Crossrail
- EC Harris
- Electrical and Mechanical Services Department, Hong Kong
- Lloyd's Register
- London Underground
- MTR Corporation Limited, Hong Kong
- RSSB, UK
- Rio Tinto
- Systra
- Technical Programme Delivery Group

This guidance does not necessarily represent the opinion of any of these people or organizations.

# Contents

# 1 Introduction

This Application Note (AN) is a component of the international Engineering Safety Management Good Practice Handbook, or 'iESM', for short. The handbook as a whole describes good practice in railway Engineering Safety Management (ESM) on projects. It covers both projects that build new railways and projects that change existing railways.

The iESM handbook is structured in three layers:

- Layer 1: Principles and process
- Layer 2: Methods, tools and techniques
- Layer 3: Specialized guidance

The first layer comprises one volume, Volume 1. Volume 1 describes some of the safety obligations on people involved in changing the railway or developing new railway products. It also describes a generic ESM process designed to help discharge these obligations.

Volume 2 provides guidance on implementing the generic ESM process presented in Volume 1 on projects. Volume 2 belongs in the second layer. At the time of writing, Volume 2 was the only document in the second layer but further volumes may be added to this layer later.

The third layer comprises a number of Application Notes providing guidance in specialized areas, guidance specific to geographical regions and case studies illustrating the practical application of the guidance in this handbook.

The structure of the handbook is illustrated in the figure on the right.

This document is Application Note 4. It supports the main body of the iESM handbook by providing guidance on Independent Assessment activities.

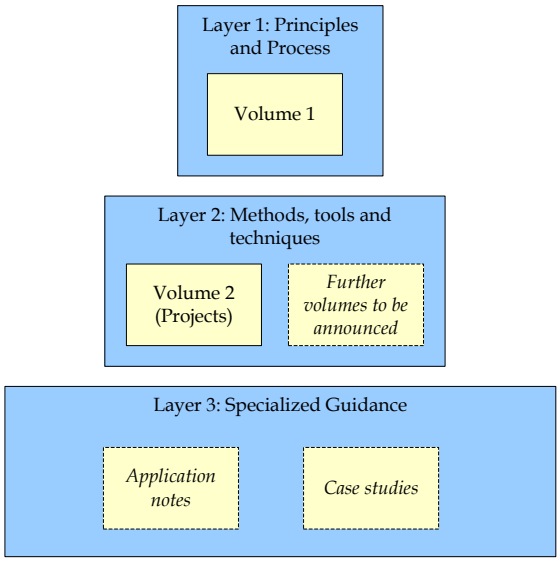


**Figure 1 The Structure of iESM Guidance**

The role of iESM Application Notes is to develop more detail where required under the existing principles and guidance in iESM Volumes (layers) 1 and 2.

# 2 Scope

The relevant iESM principle is:

"Your organization must ensure that engineering safety management activities are reviewed by competent people who are not involved with the activities concerned."

iESM Guidance Volume 2, Chapter 17 has more detailed guidance covering:

- Assessment of risk controlled by the application of standards.
- Assessment of risk not controlled by the application of standards.
- Safety audits.

Independent Assessment can also cover the full scope of EN50126/IEC62278 [50126] including Reliability, Availability and Maintainability. In many places the term used is Independent Safety Assessor or ISA. This AN is focused on that role although very similar roles are defined for an Assessment Body under European legislation or Independent Professional Review or Independent Verification / Validation elsewhere.

It is often assumed that with the right technical knowledge, planning, management and remit, people will be able to deliver effective results. While these things are necessary, they are not sufficient. This AN is primarily written for people performing Independent Assessment to help them plan their work, perform it and process observations through to supportable conclusions. The material it contains will also be useful to those who are employing an Independent Assessment organization and to Project Managers who interact with them.

Document assessment is one of the main tools and techniques that an Independent Assessor will use. There are others often used including, but not limited to, audit, Vertical Slice Analysis and test witnessing. These techniques are covered by other guidance and therefore this AN provides guidance on when and how they may be used. Much of the guidance, such as on raising observations is relevant to all tools and techniques that are in common use.

More general help is available elsewhere for the auditing element of the Independent Assessment task as it is a common process used in quality management and financial governance.

Good practice in engineering safety management advances as people build on the work done before by others. If you have any comments on this Application Note or suggestions for improving it, we should be glad to hear from you. You will find our contact details on our web site, www.intesm.org. This web site contains the most up-to-date version of this Application Note. We intend to revise the guidance periodically and your comments and suggestions will help us to make the Application Note more useful for all readers.

# 3 Guidance

## 3.1 Purpose of Independent Assessment

Independent Assessment is about building confidence that the work under assessment is acceptably safe for the application under consideration i.e. the risk is controlled to an acceptable level. A secondary purpose is to improve the ESM evidence and / or its presentation. It is not about seeking out a single, elusive "right" answer. It is about seeking improvement through a process of peer review. It is not part of the project's own verification and validation activities and should not normally repeat them. It will contribute to the final safety argument.

The Independent Assessor should be involved early on in the system lifecycle and seek to provide regular and timely feedback on the work performed by the project. It is usually easier and more cost effective to make changes to a project before physical work takes place.

Where previous Independent Assessment work has been completed and documented, it should not be necessary to repeat it. The iESM guidance provides help in applying a Cross Acceptance approach in such circumstances.

## 3.2 Independence

iESM Section 17.2.3 e) states "If you appoint independent assessors, you should ensure that they are independent of the project". Experience shows that this type of statement, which reflects the intent of CENELEC Railway Application standards, has been interpreted in different ways at various times and places.

Where projects are complex and / or novel, additional confidence in the conclusions of the assessment can be gained through increased independence of the Assessors from the Project.

Commercial independence, where the Independent Assessor works for a separate commercial entity to the Project, is international good practice for the assessment of systems with high integrity level functions (e.g. typically signalling or some rolling stock subsystems) or those products, systems or processes that can lead to a fatality. However, to avoid the possibility of an Independent Assessment organization becoming dependent on a supplier, many Regulators suggest that the Independent Assessment organization is contracted directly by the end Client. This allows flexibility to highlight safety weaknesses without suffering contractual penalties. The Independent assessment organization cannot however replace the Client role – approval is still required before a change is introduced to the railway or a new operation commences (see iESM Guidance Volume 2, Chapter 14).

Adequate independence also needs considering for individual Independent Assessors who may have changed employer and may have been involved in the

project or technology development before taking the role of an Independent Assessor.

In specific cases the Independent Assessor could be part of the same organization as the Project, but other measures must then be taken to assure safety. One possible solution is a direct line of reporting between the Independent Assessor and the Regulator or acceptance body. The Independent Assessor may be an individual or more typically a team of specialists.

## 3.3 Planning the Assessment

The Independent Assessor should work to a written plan. A typical Assessment Plan outline is provided in Application Note 2.

The Assessment Plan should be prepared at the beginning of the work and regularly reviewed and updated to address changes in the Project as well as in response to emerging assessment results. Updates should also take into account the Independent Assessor's understanding of the project risks as this could affect the competences and tasks required for the remainder of the assessment work.

It is good practice for the organization commissioning the assessment to approve or agree to the Plan.

The Independent Assessor organization should undertake a risk assessment of the Project as the first step in the planning process. For complex or novel projects, one way to do this would be to hold a brainstorm workshop. The risks identified should not be limited to the technology or design but also consider whether:

- The Project can produce a safe system.
- The Project can demonstrate the system is safe.
- The risk acceptance criteria and acceptance requirements are clear.
- The Independent Assessor team can properly assess the work.

The results of the risk assessment should be used to formulate the Assessment Plan and to identify the required competence and select the most effective types and levels of assessment activities.

The content of the Plan will be primarily driven by the remit from the Project or end Client. The Independent Assessor may work with the Project or end Client to refine the remit, and the Project should liaise with the approving authorities to agree the remit, if necessary. A typical remit is provided in Application Note 2

Assessment activities, tools and techniques should be selected on the basis of the initial risk assessment in order to:

- Collect evidence that an area presents an acceptable level of safety risk; or
- Collect sufficient preliminary evidence on an area to decide what further in-depth assessment, if any, is required.

The Assessment Plan should indicate for each assessment task:

- The purpose of the work
- The scope of work.
- The risk acceptance criteria.
- Identification of the activities to be carried out
- The purpose of each activity, and specifically what evidence will be sought.
- Inputs, outputs and dependencies.
- How the work will be undertaken, i.e. tools and techniques.
- The resource to be used, i.e. who will carry it out
- The timeframe for the work.
- Interfaces for the tasks, and any additional inputs or outputs required for the task.

The Plan should ensure that adequate emphasis is placed on assessment of technical deliverables, supported by process assessment and audit. The Plan should scope the assessment according to the remit. For example, the assessment of Operations and Maintenance manuals may, or may not be required.

The Plan should also detail how observations from each assessment activity will be recorded, categorized and to whom the feedback will be directed.

Assessors should plan for the regular review of project assumptions, dependencies and caveats during the assessment work to check they remain reasonable and are being addressed in a timely manner.

Assessors should ensure that their assessment activities are planned so as to support the Project constructively and minimize the disruptive effect on the Project. For example, the Independent Assessor could liaise with other project auditors to combine visits.

The delivery of independent assessment services should be managed like any other engineering project to ensure completion to time and to budget, and therefore the Independent Assessor should produce an overall schedule, defining:

- When each activity will be carried out, and their dependencies;
- Key milestones in the assessment;
- Dates for the issue of Project and Independent Assessor deliverables; and
- Date for completion of the assessment.

Assessment Plans should include progress reporting and regular progress meetings with the Project.

Assessment Plans should ensure adequate provision for managing Independent Assessment subcontractors.

Assessment Plans should define the observation severity categorization scheme to be used. iESM provides guidance but this can be customized to suit the needs of the

Client and the Project. Differentiation between at least major / minor is strongly recommend.

## 3.4 Staffing and Competencies

A competent person or team requires a number of qualities and capabilities, generically categorized as follows:

- The domain knowledge - empirical, scientific or a blend of both.
- The experience of the application (knowing what works and why) in different contexts, based on previous project experience.
- The drive and motivation (physical and psychological) to achieve the goals and to strive for betterment/excellence.
- The ability to adapt to changing circumstances and demands by creating new know-how to get the job done.
- The ability to perform the requisite tasks efficiently and to minimize wastage of physical and virtual resources.
- The ability to listen and determine what is desired and to deliver it consistently and with integrity, tact and respect.
- Knowledge and experience of application of Independent Assessment tools and techniques.

Note that these competences required are both technical or process, because the assessment organization also needs managerial and social skills for planning, control of meetings, negotiating and the ability to defend their position in a firm, but non-confrontational manner.

An Independent Assessor team profile should be maintained as part of the Assessment Plan. The team profile should include or refer to:

- The competency requirements identified
- Team organization chart; this should clearly show the line of safety responsibility, indicating who the Lead Assessor is.
- Copies of team member CVs, and records of their competence.
- Competency Profiles cross referenced to competences required for the Independent Assessment activities identified.
- Training records, if any specific training has been undertaken specifically for the assessment.

The Independent Assessor team profile should also include the same details for any subcontractors used.

The Lead Assessor is a key appointment. The Independent Assessor organization should ensure that Lead Assessor has the necessary competencies and has the ability to lead a team of Assessors. For large Independent Assessment projects it is often

better to appoint a dedicated Project Manager. This allows the Lead Assessor to focus on the assessment work.

Assessors should work as a team wherever possible, although not duplicate work for the sake of it. Team working offers a variety of benefits which encourage:

- A diversity of viewpoints from a team approach which can add confidence to assessment results.
- Reduced risk of the Independent Assessor not delivering to plan by avoiding over-reliance on an individual assessor.
- Reduced risk of Assessors focusing on personal areas of interest at the expense of other issues.
- Mentoring of less experienced staff and developing new Assessors as Clients may be comfortable with less experienced staff given adequate levels of supervision.

Within the team it is good practice for one person reviews a suite of documents, e.g. that person does all the hazard analysis documents.

On larger, complex projects more than one Independent Assessor organization may be involved. Some projects will require the appointment of an organization to perform a standards compliance check (e.g. a Notified Body in Europe). In these situations, a single organization should be appointed as the lead to form the single point of contact for the Client. The other Independent Assessor organizations involved then interact with the Client via the lead organization.

## 3.5 Writing Observations

Writing observations requires care with the use of language. Each Observation should be unambiguous and supported by evidence or by reference to a clause in a relevant standard. Observations should be objective and the Independent Assessor is under a professional obligation to be fair and reasonable. Sometimes observations will have an element of subjectivity in which case they should be explained fully. The purpose of raising an Observation is ultimately to reduce risk. A secondary purpose is to improve the ESM evidence or its presentation.

The Independent Assessor should guard against offering an alternative approach that suggests "your way is good, but mine is better". The role of the Independent Assessor is to consider what is presented, not what they would like to see. In most cases there is more than one safety argument that can be made.

The Independent Assessor should be aware of invisibility. There may be things that are not mentioned, or deliberately omitted, that are critical to the safety argument. A checklist against the requirements of the relevant standards can help but some of these issues will be contextual to the specific project. Where things are missing the Independent Assessor should raise an Observation but be wary of stating a solution.

In general, the Independent Assessor should avoid suggestion fixes and changes, although the provision of general guidance is good practice. An Independent Assessor that resorts to dictating an approach risks compromising their independence.

The Independent Assessor should avoid using the observation management process for seeking information from the project that can be obtained another way. Projects may have a Request For Information (RFI) system or else a simple request will be more effective.

When documents have been written in a language that is not the mother tongue of the author there may be clumsy phrases or poor grammar. It is not good practice for the Independent Assessor to focus on this unless there is a clear safety impact through ambiguity. If the intent is clear then raising an Observation just creates more work for the project and the Independent Assessor.

The documents to be assessed will vary by project. There are likely to be some significant safety engineering deliverables (e.g. System Safety Plan, Quality Plan, Safety Case) that are commonly required by Clients and published standards. These should be closely examined as should their supporting (child) documents. It may be more practical to provide observations on these major documents rather than raise the same, or similar issues, on several related ones. Consistency and referencing between the documents and their various versions is important to consider.

## 3.6 Managing Observations

The three part form described in iESM Guidance Volume 2, Chapter 17.2, paragraph g of the iESM guidance is often referred to as a Safety Notice. It should be given a unique reference and issue number. The Lead Assessor, or his delegate, should review and approve all Safety Notices before issue. There may be one Safety Notice per document reviewed or more usually one per main deliverable with other documents that are examined identified as supporting material.

Each Observation should also be given a unique serial number for traceability.

When a particular Observation is responded to by the project, the response can usefully be recorded in the Safety Notice. To achieve this, the Independent Assessor will need to issue an editable form of the Safety Notice in parallel with a secure version containing signatures.

The Safety Notices should thus form a complete, auditable record of the observations, the Project's responses and any closure comments or actions that arise.

## 3.7 Classifying Observations

Classifying observations requires skill and judgment built up through experience. The framework for classification is defined in the Assessment Plan, however its

application is subjective. It is not something that can be learnt from an Application Note. There are however some general principles to use in conjunction with the suggested scheme in the iESM Guidance Volume 2, Section 17.2, paragraph g:

- The highest categorization of observation should be used sparingly. If the initial assessment is that here are many high category observations it would be better for assessment to be stopped until the document is in a better state.
- The lowest category of observations should be grouped if possible. They may reflect poor validation processes within the project and so their impact should be considered.
- A quantity of medium category observations may be indicative of a poorly run project or lack of precision. The Independent Assessor may consider raising a combined high category Observation in such a case. This should however be considered a last resort.
- A missing hazard is a fundamental weakness and should be raised as a highest category observation. The Independent Assessor should make sure that they have correctly understood the boundary and function of the system first.

## 3.8 Reviewing Project Responses

There can be a feeling of teacher-pupil between the Project and the Independent Assessment organization (in either direction) which may be unhelpful. There are many ways to make and support a safety argument and the Independent Assessor's role is not to enforce their own preference as if they were in a senior role. The Independent Assessor, if they are professional, will raise observations for good reason and should expect that they will be responded to in a calm and reasonable way. If an underlying conflict is detected then this should be dealt with outside the observations management process – usually through a discussion. Responses by the Independent Assessor and the Project should:

- Be clear and to the point.
- Make sure the entire Observation or response is considered and addressed.
- Challenge the response, if necessary, but attempt to anticipate the reaction by providing a full justification and explanation.
- Identify clearly if a change is needed to the document under assessment, other documents or artifact.
- Identify clearly if a change is needed to a physical artifact.
- Consider the impact of the change on other parts of the document or other documents.
- Refer to other Observations or responses where it is does not degrade readability.

- Ensure that agreed changes are made in the affected documents or artifacts with suitable revision records and re-issue them.
- Avoid point scoring

In reviewing the project responses the Independent Assessor should make it clear whether they accept them or still seek further evidence or clarification. Based on the response it is reasonable to reclassify an Observation without closing it if its impact has been mitigated by the project.

It is not good practice to raise further points on the Project's responses unless the point can be dealt with simply. It is almost always better to raise a new Observation which can be managed in its own right.

A "Letter of Concern" can be used to escalate observations which the Project are unwilling or unable to address themselves. Examples may include:

- Inadequate response or untimely delay in responding to observations.
- Perceived ineffectiveness of remedial actions.

Letters of Concern can be useful but should be considered a last resort and only where the emerging safety properties could be expected to be compromised. If that remains the case, the Independent Assessor will not be able to recommend that the Project be brought into use (or where applicable continue in use).

## 3.9 Producing an Assessment Report

A typical Assessment Report outline is provided in Application Note 2. Reports may be produced at each significant phase or milestone and will support any certificate issued. The Assessment Report should set out the approach adopted by the Independent Assessor, justifying any deviations from the agreed Assessment Plan.

It should set out the Independent Assessor findings, considering the scope and purpose of the work, on the review of the ESM process and safety deliverables. It should confirm, or not, that the Project's safety argument and supporting evidence assessed is adequate for the application under consideration or the conclusion of that phase of the development.

Preliminary Assessment Reports may be issued if it is not possible to perform all the safety activities prior to the commissioning, e.g. it may not be possible to perform all measurements or tests prior to the commissioning.

## 3.10 Independent Assessment Certification

Many railway administrations and regulators will have their own mandated form of certificate. The standards EN45011/ISO Guide 65 provide guidance for certificate issuing bodies. Independent Assessment organizations may be accredited against these standards. If no specific guidance is available the following is good practice:

- Unique identifier for the certificate
- Independent Assessor organization name and address
- The artifact to which the conformity statement relates is specified. This means a statement of what is certified, e.g. a product, system or process and in the case of new product, the lifecycle phase covered.
- The specification of the artifact should be clearly stated (e.g. a specific configuration baseline or a software version). For a technical change, a unique and unambiguous identifier should be given and a list of the specification documents such as drawings, should be given in a schedule or annex to the certificate.
- Dates of issue and expiry, if relevant.
- Reference to the Assessment Report(s) in which the conduct of the assessment and the supporting evidence are recorded
- Limitations and qualifications (temporary or permanent) to the assessment which may be in an annex to the certificate

A list of signatories authorized to sign certificates on behalf of the Independent Assessor organization should be maintained.

Letters of Support are sometimes used in place of a formal certificate but they should still contain the key elements required and be managed in a robust an auditable way.

After a Project has been certified, any subsequent modification shall be controlled using the same quality management, safety management and functional/technical safety criteria as would be used for a new design. All relevant documentation, including the Safety Case, should be updated or supplemented by additional documentation, and the modified design shall be submitted for Independent Assessment.

# 4 Tools and Techniques

## 4.1 Overview

Independent Assessment is usually best performed through a structured series of both Safety Audits and output Safety Assessments, that is a combined of process-focused reviews and product-focused reviews. These may be supported by Vertical Slice Analysis, test witnessing or other appropriate techniques (e.g. design analysis) as needed on a specific Project.

Product-focused reviews provide evidence as to whether or not the risk associated with the Project is (or will be) reduced to an acceptable level.

Process-focused reviews or audits provide evidence that Safety Plans, procedures and standards are being followed.

The activities of the Independent Assessor should include:

- Review of the adequacy of the safety requirements and the Project's ability to fulfil them.
- Review of the Project safety and quality organization.
- Review of the ESM processes and their outputs, specifically the Project Safety Plan, the Hazard Log and the Safety Case(s).
- Compliance with standards, where applicable.

## 4.2 Performing a Safety Audit

Auditing is covered extensively by other guidance. There are no special requirements for safety auditing apart from the focus of the work and the competence of the people performing it.

Safety Audits are intended to check that the ESM is adequate and has been carried out in conformance with a suitable Safety Plan or other nominated standard. A Safety Audit should consider:

- Work since the previous audit (all work so far, if first audit).
- Plans for the next stage.
- Observations from the previous audit.

It is good practice for the Safety Auditor to prepare an audit checklist to guide enquiries and to record results and evidence. The format of the checklist should mirror that of the Safety Plan and associated ESM activities such that each aspect of these is directly addressed by a question in the checklist. It should be in the form of a checklist with questions that may be answered 'Yes' or 'No'.

The checklist should be drawn up to meet the audit requirements, using the documents referenced in the remit. The Safety Auditor should also note anything that they find that is objectively wrong, whether or not it relates to a checklist item.

Note that the checklist is an aid for the Safety Auditor – it should not be completed by the Project.

The Safety Audit should check that any standards or procedures called up by the Safety Plan have been correctly applied. It should also check that there is traceability from the Safety Plan to project activities that implement it.

The Safety Audit should look for documentary evidence that every safety-related activity has been carried out in accordance with the Safety Plan, or otherwise justified, without any blocking issues being identified. The answer to each question on the audit checklist should be supported by documentary evidence. Instances where there is no evidence of compliance should be documented along with a recommendation for remedial action. Each non-compliance should be identified in terms of the specific requirements of the Safety Plan. The Safety Auditor should classify the significance of each finding.

Information gathered through interviews should, where possible, be verified by acquiring the same information from other independent sources.

The primary output of an audit is a Safety Audit Report. This report should include:

- A judgement on the extent of the project's compliance with the Safety Plan.
- A judgement on the impact of any non-compliances.

If the Safety Audit results are unsatisfactory, then it may be sensible to postpone other Independent Assessment activities until corrective action has been taken.

One of the positive outcomes of a Safety Audit can be the opportunity to share good practice through their findings, without the Independent Assessor specifically recommending certain actions.

## 4.3 Performing a Document Assessment

Before beginning an assessment of a document, the Independent Assessor should consider carefully what they expect to find, based on their own experience and the previous deliverables, including the System Safety Plan, from the project. As soon as the Independent Assessor begins to read the document they will begin to be led by the author down a predetermined path towards an expected conclusion of agreement with the author. This is not necessarily wrong, but can be unhelpful when the Independent Assessor needs to be looking for omission or weakness in the evidence or safety argument. It is also important to establish early on that the document is fit for review – that it has been through the Project's review and approval processes and contains the expected material.

The Safety Assessor should become familiar with the:

- Hazard Log.
- Project Safety Plan.

- Safety Requirements Specification.
- Findings and recommendations of any previous Safety Assessments or Safety Audits.
- Project progress and status.

Document assessment is often effectively performed on a theme e.g. hazard management, ESM planning. There may be one main document under review but several supporting documents will be reviewed for their contribution.

The following basic checklists may help in ensuring adequate coverage:

Content:

a) Is there a clear statement of objective?
b) Is the scope clearly defined and is it self-consistent and consistent with earlier deliverables?
c) Has the specified ESM process in the Project Safety Plan been followed?
d) Have risk acceptance criteria and safety requirements been defined / met?
e) Is there a clear statement of conclusion relative to the objective?
f) Is there necessary and sufficient evidence to support the conclusion?
g) Are outstanding issues or residual risks clearly identified?
h) Are there recommendations relating to further work or outstanding issues?
i) Were there specific outputs arising from audits that need to be assessed?

Presentation:

a) Is the document correctly signed off?
b) Has the specified configuration management been applied?
c) Are changes since the last version clearly identifiable and explained?
d) Is the document complete including appendices?
e) Are the headers, footers and other identification marks consistent throughout?
f) Is the content appropriate in terms of style, volume and presentation for the objective of the document?

In terms of reducing risk it is the content that is most likely to influence the outcome. However is the presentational items are neglected it can be hard to gain confidence in the work under assessment and time will be wasted. All observations should be peer reviewed within the Independent Assessor organization before they are released to the project.

In performing the assessment, the Project requirements for Reliability, Availability and Maintainability (RAM) should be considered. Whilst they are not the subject of the assessment, the design decisions made in achieving cost and capacity requirements may dominate. The Independent Assessor should clearly identify any conflicts and consider the need for trade-off studies, design or operational reviews to

identify and implement optimised solutions which maintain the level of safety achieved.

## 4.4 Test Witnessing

Witnessing tests can provide confidence to the Independent Assessor that the Project is well managed and that the emerging evidence of meeting the safety requirements will be dependable. However, on most projects it will not be possible to witness all the testing. A sample will therefore need selecting which is representative of the critical tests which demonstrate specific safety-related properties of the Project.

On some projects it will not be possible to gain confidence from witnessing a final acceptance test, however comprehensive it is and it will be necessary to witness unit and integration tests, or samples of these tests.. These activities, carried out as Project proceeds, aim to ensure design integrity and compliance with standards and procedures.

The following guidance may be helpful:

- Completely understand the tests to be witnessed.
- Accommodate the Project's schedule to avoid possible delays.
- Review all test documentation before the tests.
- Review the purpose of the tests, any associated procedures and any limitations of the test scenario (e.g. simulation) with the Project prior to commencing the tests.
- Agree which tests are of particular importance so the Project can give them extra attention.
- Understand the test scenarios as they may involve simulation of interfaces or data.
- Understand how to interpret the results and how they impact on the outcome of the testing (e.g. the pass/ fail criteria) .
- Check who is performing the tests, their competence to do so and their independence.
- Allow sufficient time for tests. Some tests may require a long set up and very little execution time. Others, such as taking temperature readings, can last overnight.
- Consider the need for regression testing if changes or re-work has been made.
- Check that states for start-up, steady-state (normal operation), shut-down, maintenance and abnormal operation are addressed.
- Conduct a physical inspection of the equipment, using the following checklist as a guide:
    - Connections and grounding positions are robust and correct.
    - Name plates, warning labels, colour etc. are correct and in an easily readable position.

- Gauges, displays and monitors are positioned for readability and accessibility.
- Serial numbers of test equipment, versions of software, firmware and hardware are recorded.
- Test equipment calibration and expiry dates.

Often ad-hoc testing by the Independent Assessor or, on their behalf can provide additional confidence or highlight unexpected system behaviour. Ad-hoc testing, sometimes called "free hand" or "exploratory" testing starts with a documented test procedure but without a pre-prepared script, introduces additional improvisations as the test progresses based on emerging responses. It is a functional test where the tester attempts to "break" open the system's functionality, perhaps by creating realistic, but unlikely, scenarios. Although it is unscripted it is important that the tester keeps track of exactly what they are doing in order to reproduce any behaivior identified.

## 4.5 Inspections / Examinations

Sometimes it is useful for the Independent Assessor to carry out some inspection of the completed artefacts or major sub-systems to add confidence that they are free from obvious defect. The purpose of visual examination is to identify any problems that are likely to affect integrity. The configuration arrangements and baselines for the parts necessary to ensure safety can also be confirmed. An inspection may include:

- Visual examination
- Dimensional examination
- Functional or operational test or witness
- Open-up examination
- Electrical test and examination
- Non-destructive test

## 4.6 Sampling Guidance

Sampling may be necessary or sensible for all of the tools and techniques, in particular auditing and test witnessing. The objective of sampling is to enable the Independent Assessor to gain an appropriate level of confidence in a specific area when assessing all the related evidence is not practical. This can often arise in the case of well-defined engineering processes which generate large volumes of records.

Any sampling should be based on expert judgement informed, where appropriate, by ISO2859 [2859]. Whereas the theory indicates that the samples should be selected at random by the Independent Assessor, it is more appropriate to select items that are likely to be more material to controlling the most significant risks. The objective and rationale behind any sampling should be defined and documented. Should the

sampling reveal significant problems then further, more extensive, review should be performed.

In deciding whether sampling is appropriate, the Independent Assessor should restrict sampling to those areas where:

- Multiple documents are produced with essentially similar content and purpose.
- Each document makes broadly a similar contribution to compliance and safety.
- Areas that are repetitive in nature.

The following typical examples of what is appropriate or not are intended to add greater clarity, not prescription.

The areas where samples are unlikely to be permissible include:

- Grouping dissimilar specification together to produce a significant sample size e.g. hardware specification, software specification, interface specification,.
- Critical documents such as Safety Plan, Validation Plan

The areas where examination of samples is likely to be permissible include:

- Module specifications (where several software modules at the same level are being specified).
- Test logs for a particular test or for low level tests, test logs at the same level
- Drawings.

# 5 Glossary

This glossary defines the specialized terms and abbreviations used in this Application Note.

## 5.1 Abbreviations

| | |
|---|---|
| ESM | Engineering Safety Management |

## 5.2 Specialized terms

| | |
|---|---|
| Assumption | A statement that is taken to be true and relied on, even though evidence for its truth is not yet available |
| Caveats | Conditions that people must respect after the change is put into operation for it to remain safe. |
| Dependency | An agreement between the project and another party that something will be in place before the implementation of the change |
| Engineering Safety Management (ESM) | The activities involved in making a system or product safe and showing that it is safe.<br>Note: despite the name, ESM is not performed by engineers alone and is applicable to changes that involve more than just engineering. |
| Hazard | A condition that could lead to an accident. A potential source of harm. A hazard should be referred to a system or product definition. |
| Project | The planned change to the railway or development of a new product, system or process. |
| Safety Notice | A formalization of the three part form that allows tracking and closure of observations |
| System | A set of elements which interact according to a design, where an element of a system can be another system, called a subsystem and may include hardware, software and human interaction. |
| System lifecycle | A sequence of phases through which a system can be considered to pass.<br>A product may also pass through some of these phases. |

# 6 Referenced Documents

This section provides full references to the documents referred to in the body of this document.

[YB4] *Engineering Safety Management, issue 4, "Yellow Book 4"*, ISBN 978-0-9551435-2-6

Yellow Book 4 now has the status of a withdrawn document.

[2859] ISO2859:2002, Sampling Procedures for Inspection by Attributes.

[50126] EN 50126, *Railway applications – The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS). Also issued as IEC62278.*

*At the time of writing the current issue of EN 50126 was dated 1999 but the standard was being revised to cover the scope of EN 50128 and EN 50129 and other railway systems. As far as we can, we have aligned this guidance with the emerging issue. If an issue of EN 50126 dated later than 1999 is available at the time of reading then this issue should be consulted. If no issue of EN 50126 dated later than 1999 is available then the reader may find it useful to consult the current issues of EN 50126 and EN 50129 but may not find the information referred to in any particular citation of the standard.*

# iESM

international Engineering Safety Management

Good Practice Guidance
Application Note 4

Published on behalf of the International Railway Industry
by Technical Programme Delivery Ltd