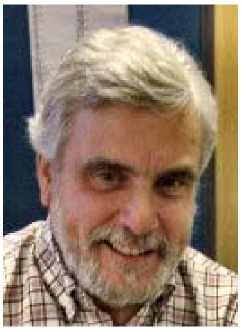
INDEPENDENT VERIFICATION AND VALIDATION (IVV) ON RAILWAY PROJECTS

By Eric S. Long – Consulting Engineer & Associate Consultant to PMSC



Dr, Eur-Ing Eric S. Long is a graduate of the Universities of Manchester and Salford, majoring in Mechanical Engineering and Advanced Manufacturing Technology and Management. He undertook his initial training at Metropolitan-Vickers in Trafford Park, Manchester, followed by extensive experience in research, consultancy and at one of the foremost inspecting authorities in Europe. Eric is a Chartered Engineer, an independent Consulting Engineer specialising on the Development and Auditing of Safety and Reliability Management Systems, and a Visiting Professor of Safety Law

CONTENTS OF PAPER

Abstract

The following article highlights the major elements to be considered when undertaking an Independent Verification and Validation Study – providing an overview of the Auditing and Management procedures over RAMS during the Systems Assurance Evaluation throughout the design stages of a railway project. The article is based essentially upon the requirements and the author's interpretation of EN50126, which has become the principal standard to be adopted for the life cycle Systems Assurance of any railway project. Whilst the author has had specific experience in carrying out an Independent Verification and Validation Study of a high speed railway in Asia, together with Metro Systems, the article is presented in a generic style, and therefore could be adopted on both high speed railways and light rapid transport systems, together with underground rail networks.

Copyright

Section 1.0 Introduction

The Standard of control for the Systems Assurance process that is now being employed during the whole life cycle of a railway project is EN 50126 1999: Railway Applications – The Demonstration and Specification of Reliability, Availability, Maintainability and Safety (RAMS). This Standard provides details on the requirements of the Systems Assurance process during Design, Construction, Installation, Operation and Decommissioning – ie throughout the whole life cycle of the railway project. The following article endeavours to explain some of the key issues of the Standard, along with the author's interpretation during its use on a major railway project.

Some of the issues that are covered include:

- Definitions and interpretation of the terminology used
- Details of the structure of the Standard in terms of the phases throughout the life cycle of the project
- Interpretation of the requirements of the Standard in so far as the design phases are concerned, including essential requirements and mandatory elements of the Standard
- General management support that is required in order to fulfil the recommendations of the Standard
- Advice on the development of a Safety and Reliability Management System in order to ensure a structured approached to verifying and validating the RAMS design
- Independent verification and validation in the context of Peer Review, and the key role of Auditing the process and documentation deliverables.

The article concentrates on Phases 1 to 6 of the Standard, incorporating the conceptual, preliminary and definitive design stages of a typical rail project

Section 2.0 Definitions of Terminology Used in the Article

It is important to have a thorough understanding of the terminology, before progressing onto the process of verification and validation. The definitions of verification and validation could essentially comprise –

- Verification – The Oxford Dictionary defines ‘verify’ as – to examine for the purpose of establishing the truth, in terms of statements, items, figures etc. The terms of Systems Assurance, the author interprets this as – the process of checking procedures to ensure that they are appropriate and adequate, in order to obtain the correct results when validated
- Validation – The oxford Dictionary again defines ‘validate’ as – to ratify or confirm the validity (of the results). Again, in terms of Systems Assurance, the author interprets this as – the process of checking that the results correspond with the targets required

In terms of EN50126, the term Verification is more narrowly defined as –

- To demonstrate that the specific inputs and the deliverables of each phase of the life cycle development, meet in all aspects the requirements of that phase, confirmed by the provision and examination of the objective documentary evidence that the specified requirements have been fulfilled. The emphasis here is on the ‘specified requirements being fulfilled’

Similarly, in EN50126 the term Validation is defined as –

- To demonstrate that the system under consideration, at any step in its development and after installation, ie throughout the whole life cycle phases of the project, meet the requirements in all aspects, confirmed by study, testing and examination of the system, to ascertain that the particular requirements for a specified intended use have been fulfilled. Again the emphasis is on the ‘particular requirements for a specified intended use’; or in other words validating the actual results achieved against the target values

It is clear therefore that the activities of verification and validation should form an integral part of the overall demonstration of Systems Assurance, and so be intrinsically linked to the development of the railway system requirements through a management control process

Throughout the article, the term Systems Assurance is used. For those unfamiliar with the term, it is defined as –

- The means by which the customer can be assured that the design of the project is safe and reliable and meets the risk and performance targets, and comprises of various RAMS techniques (not covered in this article)

- For completeness, the term RAMS is an acronym referring to Reliability, Availability, Maintainability and Safety. Sometimes the ‘S’ refers to Supportability (ie spares logistics), which compliments the term ‘Maintainability’. In the author’s opinion this is more sensible, as ‘Safety’ is of such paramount importance that is should not be tacked onto the end of

‘RAM’, giving the appearance of some secondary element to that of ‘RAM’, but should be separately identified in it’s rightful status

Section 3.0 Interpretations of the Terms Verification and Validation

Verification
The author’s interpretation of the above definition of ‘verification’, is that of verifying that the Systems Assurance techniques, processes and methodologies are appropriate and adequate to achieve the objectives; assessed by verifying the supporting documentary procedures, together with substantiating that the specific inputs, requirements and deliverables from such procedures for each phase of the project’s life cycle, will meet in all respects the requirements of that phase

For the purposes of satisfactory verification, there must be evidence of three key elements –

- Planning
- Control, and the
- Provision of an Audit Trail

Detailed planning of the Systems Assurance process is imperative and must form the basis of a schedule or programme against a time frame on such as a Ghant Chart. For Systems Assurance evaluations of complex or extensive systems, a critical path analysis could be envisaged. This will ensure that the Systems Assurance process for each phase in the life cycle will be achieved in a logical way, and within the time frame required. Planning will also allow a consideration of adequate levels of resource to be provided at each stage.

Control over the Systems Assurance process can only be achieved by the generation of planned procedures. Such procedures form a ‘standard’ of control’ and must be accepted by all parties involved in the Systems Assurance process and by the customer. Only by creating such standards of control, can we ascertain that the requirements and deliverables will be met, and to facilitate the auditing and management of the process (See below for more details on the so-called ‘standards of control’).

The provision of an audit trail is imperative for the identification and traceability of all the Systems Assurance decisions made during each phase of the project. This will facilitate any backtracking of the Systems Assurance process where there are any shortcomings in the deliverables from any phase.

Validation
Again, the author’s interpretation of the above definition of ‘validation’, is that of validating that the system, so designed and constructed, meets the acceptance criteria and requirements for the system; achieved by ratifying the results of Systems Assurance studies, and by witnessing the tests and examinations of the system, in order to confirm that the deliverables at a particular phase of the life cycle meets the targets for the system under consideration, as being ‘fit for purpose’

The emphasis here is on ratifying results and witnessing tests that demonstrate the performance of the system against the acceptance criteria in the customer's technical specification

Section 4.0 Aims, Objectives and Benefits of Adopting EN50126

The aim of the Standard is to:

- Enable a structured review of the management control over the RAMS design process, and
- To be aware of the RAMS application to the design of the system, taking account of: (a) the cost of system development, and (b) the ultimate cost of ownership of the system – with reference to Economic Life Cycle Costing'

The objective of the Standard is to:

- Provide a consistent systems approach to the management of RAMS, and
- Aim to promote co-operation between all parties

The benefits of the Standard are to:

- Act as an aid to defining the interaction between the elements of RAMS throughout the life cycle of a project
- Address any conflict between the RAMS elements (see Safety and Availability below)
- Specify the requirements for RAMS inputs and deliverables at each phase of the project, and
- Provide a framework to demonstrate that RAMS procedural requirements are being met and sustained
- Standard itself is not mandatory, and the requirements of the Standard are as such 'recommendations' – reference section on Mandatory Elements of the Standard below

The Standard is based upon tried and tested recommendations from the railway industry.

The Standard does not:

- Define RAMS targets, or the quantification of such targets, nor
- Stipulate the RAMS requirements, methodologies, techniques or solutions

The Standard, understandably gives priority to safety as opposed to RAM

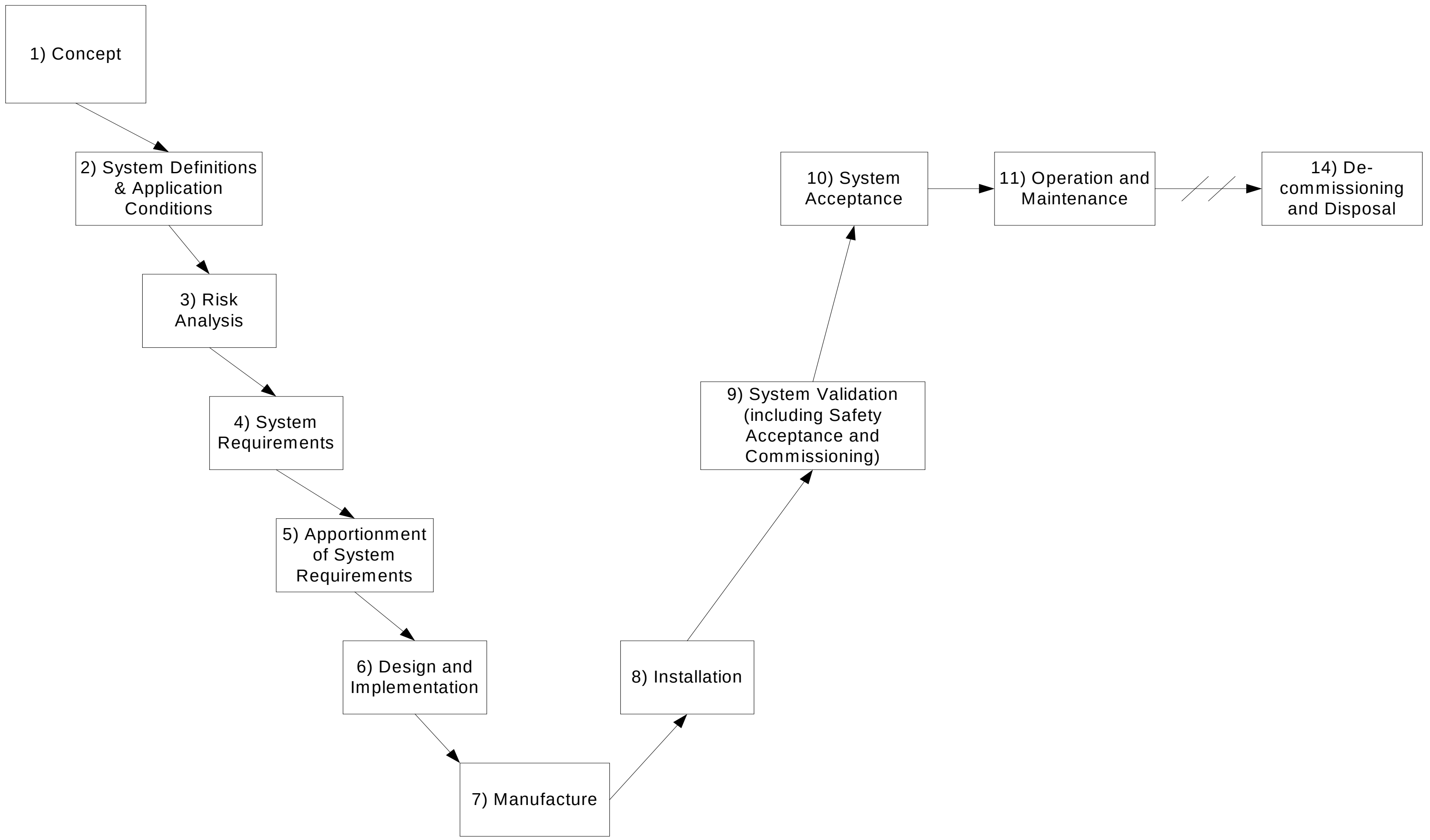
Section 5.0 Details of the Phases in EN50126

The Standard comprises 14 phases, including –

- Concept
- Systems definition and application conditions
- Risk analysis
- System requirements
- Apportionment of system requirements
- Design implementation

- Manufacturing
- Installation
- System validation (including safety acceptance commissioning)
- System acceptance
- Operation and maintenance
- Performance monitoring
- Modification and retrofit, and
- Decommissioning and disposal

Whilst the phases are linear in concept, RAMS is an iterative process, and out of necessity there will be a degree of overlapping of some of the above phases


1) Concept
2) System Definitions & Application Conditions
3) Risk Analysis
4) System Requirements
5) Apportionment of System Requirements
6) Design and Implementation
7) Manufacture
8) Installation
9) System Validation (including Safety Acceptance and Commissioning)
10) System Acceptance
11) Operation and Maintenance
14) De-commissioning and Disposal

Section 6.0 Mandatory Elements of EN50126

Where the Standard is adopted, the following are considered to be mandatory elements –

- Define and agree responsibilities for carrying out RAMS tasks within each phase, in the form of a management structure
- Define and agree the interfaces between the associated RAMS tasks
- RAMS personnel to be competent to discharge their responsibilities
- Establishment and implementation of the Safety Plan and RAM Programme
- Addressing any conflict between safety-focussed tasks and RAM cost-driven tasks
- Standard's recommendations to be supported by, and implemented within, the company's established Quality Management System
- Configuration Management System to be established and implemented, addressing all RAMS tasks – to provide a basis of control over the development of the baseline design, and for essential traceability of design decisions. Configuration Management to comprise: (1) Organisation and responsibilities for RAMS design, (2) Change management procedures and control over baseline changes, (3) Registration of changes and maintenance of register, and (4) Accurate record keeping of design changes, including (a) change request approval procedures, (b) timescales for approval, and (c) pricing and cost/ benefit analysis of baseline design requests

Section 7.0 Management Support for Implementing EN50126

The Standard cannot be adopted and applied to the RAMS design process completely in isolation of the company's existing management controls, and as such it must be supported by what the author terms 'Peripheral Controls' and 'General Management Procedures', viz –

- Hierarchical management structure
- Communications management network and lines of communication
- Quality planning
- Interfacing between engineers regarding the design interface issues of sub-systems
- Design approval procedures
- Procurement controls
- Effective project management
- Control over contractors and suppliers
- RAMS to be integrated with existing design knowledge base in the company

Section 8.0 Safety Management System of Control over EN50126

Safety particularly must be generated from within the organisation and driven by senior management, not 'bolted-on' by an outside authority. As such, RAMS management and control must be integrated into the existing management structure for effective control of safety at all phases in the life cycle of the project; and verified and validated to EN50126 by an independent department or authority. In order to accomplish this integrated approach the company must have a developed and installed Safety Management System to: (1) integrate RAMS design and control procedures into the existing management structure, and (2) to monitor, record, review, audit and assess the design process as a part of providing a continuous measure of configuration management control in the form of a 'closed loop system'. Effective verification and validation will not be accomplished without an effective Safety Management System of control, and the above two control elements of the Safety Management System are essential in order to verify and validate the RAMS design process and the results against the target values, respectively

The Safety Management System must be 'robust' to cover a flexible approach, and essentially comprise:

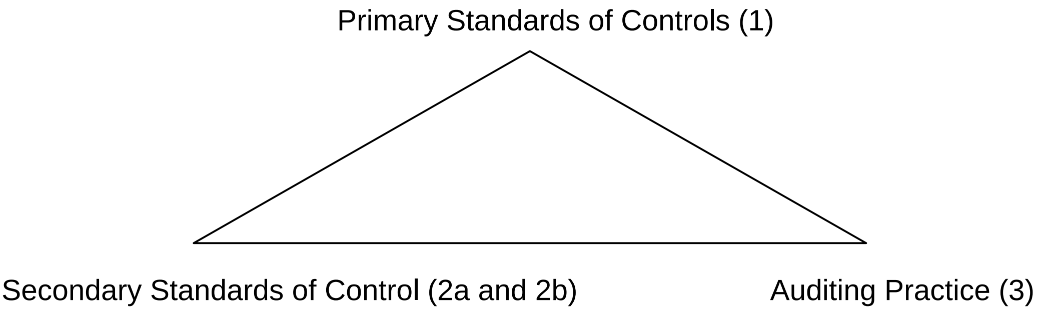
- Policy of commitment by senior management
- A 'system' boundary required to be controlled, along with interfaces with the 'system'
- Management hierarchical structure, including responsibilities, lines of accountability and competence levels (Suitably Qualified and Experience Personnel - SQEPs)
- Inputs required to the system
- Processes and procedures
- Communications network
- Controls over processes and procedures
- Level of supervisory control depending upon the complexity and scale of the process

Generally speaking, auditing against the Safety Management System will identify 'non-compliances' against established management procedures, and assessment will identify 'non-conformances' against target values. Interpretating the above terms: 'non-compliance' refers to deficiencies and failures in the organisational and procedural management control, against a recognised and accepted standard of control or system of work; and the term 'non-conformance' refers to deviations in the product design when assessed against a quality or technical standard

Section 9.0 Planning and Control during Initial Stages of EN51026

It is extremely important that a Verification and Validation Plan is developed at the initial stages of the project and not left until the preliminary design is nearing completion. The Plan should mirror the RAMS evaluation programme and schedule of work. Typically, the V&V Plan should encompass a review of the following elements –

Triangle of Auditing Control


Primary Standards of Controls (1)
Secondary Standards of Control (2a and 2b)
Auditing Practice (3)

Supported by –
Peripheral Standards of Control (2c)

All Supported by – General Management Procedures (2d)
Within the framework of a –Safety and Reliability Management System (2e)

(1) Primary Standards of Control:
EN50126, Customer Technical Specification, and SHE Legislation

(2a) Secondary Standards of Control – Upper Level:
System Assurance Plan (SAP)

(2b) Secondary Standards of Control – Lower Level:
Detailed System Safety Assurance Plan (SSAP), and Detailed Reliability, Availability, Maintainability Assurance Plan (RAMAP)

(2c) Peripheral Standards of Control:
Configuration Management, Design Change Management, Systems Interface and Integration Management, and Approved Documentation Control

(2d) General Management Procedures:
Quality Management System and Communications Management

The Secondary Standards of Control, Upper Level (2a) and Lower Level (2b) have been generated directly from the Primary Standards of Control (1), above. The Secondary Standards of Control (2a and 2b), should be supported by Peripheral Standards of Control (2c) and General Management Procedures (2d), above. The Secondary Standards of Control, including the Peripheral Standards and General Management Procedures (2a, 2b, 2c, and 2d), must be activated within a Safety and Reliability Project Management System (2e)

The so-called ‘Triangle of Control’ comprises Auditing compliance with the –

- Secondary Standards of Control
- Peripheral Standards of Control
- General Management Procedures, and
- Safety and Reliability Project Management System

Now the Secondary Standards of Control become the main compliance control documents. By Auditing the Secondary Standards of Control (ie the link between [3] and [2a and 2b] above) for compliance, we are assured that the Primary Standards of Control are being met at each phase of the project (ie the link between [3] and [1] above), and the correct deliverables are being verified

By Auditing the supporting Standards of Control (ie 2c and 2d, above), along with the Safety and Reliability Project Management System (ie 2e above), we are assured that the Secondary Standards of Control are being managed and executed effectively

A study of the ‘Primary Standards of Control’, such as the:

- Customer’s Technical Specification
- Legislation and Approved Codes of Practice
- BS/EN/ISO Standards
- Industry Standards

- Best Practice – applicable to the design

A study of the 'Secondary Standards of Control', such as the:

- Overall Systems Assurance Plan
- Systems Safety Assurance Plan
- Systems RAM Assurance Plan – all of which would be developed by the RAMS Team, and must incorporate all the essential elements of the above 'Primary Standards of Control'

Study of the 'Supporting Standards of Control', such as the:

- Project Management Plans
- Quality Management Plans – which sit alongside and complement the Safety Management System, providing a framework in which the RAMS design process is controlled and managed

Study of the 'Peripheral Standards of Control', such as the:

- Sub-Contracted Designer Procurement Approval and Control
- Design Approval Procedures
- Design Configuration Management Plans
- Design Change Management and Approval plans
- Communications Management Plans – etc – which form detailed procedures within the Project and Quality Management Plans, above

Note that once the 'Secondary Standards of Control' have been evaluated and approved, these now become the 'controlling' documents and the 'Standards' by which the Systems Assurance process should be carried out, and verified and validated against. This is what the author refers to as the 'Auditing Triangle of Control'

The V&V Plan will also identify the observations to be made on HAZOP training sessions for participants, the HAZOP sessions themselves, closure of identified Hazards incorporated in the design, and the creation of the Hazard Management Log and subsequent Risk Register for the project design

The V&V Plan should also identify how non-compliances will be reported and the future action that should take place

Section 10.0 Details of Requirements in Phases 1 to 6 of EN50126

The following provides a listing of the essential requirements of Phases 1 to 6, over the conceptual, preliminary and definitive or detailed design stages. Important elements where 'verification' is specifically required, are highlighted in bold (to verify) text

Phase 1 – Concept

General tasks comprise –

- Establish the scope, context and purpose of the railway project
- Define the railway project concept
- Undertake financial analysis and feasibility studies

- Establish a management structure to implement RAMS requirements

Safety tasks comprise –

- Review of previously achieved safety performance data **(To verify)**
- Consider the safety implications of the project
- Review of the safety policy and safety targets

RAM tasks comprise –

- Review of previously achieved RAM performance data **(To verify)**
- Consider the general RAM implications for the system/ project

Combined RAMS tasks comprise –

- A design policy to focus on and incorporate safety and reliability issues throughout the design process
- Acquiring an understanding of the environmental considerations, such as -
  (1) Potential systems interfaces
  (2) Environmental noise and vibration
  (3) Physical issues
  (4) Social/ cultural issues
  (5) Political issues
  (6) Legislation
  (7) Economy **(To verify)**

In addition to which –

- Identify sources of hazards, which could affect RAMS performance, such as interactions with other railway systems and human beings **(To verify)**
- Assess the adequacy of the methods, tools and techniques used within this phase **(To verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with any assumptions and justifications

<u>Phase 2 – System Definition and Application Conditions</u>

General tasks comprise –

- Establish a mission profile, including –
  (1) Performance requirements, including life cycle costing RAMS targets
  (2) Long term operating strategy and conditions
  (3) Long term maintenance strategy and conditions
  (4) System life cycle conditions, including life cycle costing
  (5) Logistic considerations
- Prepare system description
- Identify operation and maintenance strategies
- Identify operating conditions and maintenance conditions
- Identify any influence from existing infrastructure constraints

Safety tasks comprise –

- Evaluate past experience data on safety
- Perform a preliminary hazard analysis, including –

(1) Identify sub-systems associated with identified hazards
(2) Perform a hazard identification process **(To verify)**
(3) Identify types of accident-initiating events, including component failure, procedural faults, human error, and dependent failure mechanisms

- Establish an overall safety plan **(To verify – including adequacy of data sources included)**
- Define the tolerability of risk criteria
- Identify the influence on safety of the existing infrastructure constraints

RAM tasks comprise –

- Evaluate past experience data for RAM
- Perform a preliminary RAM analysis to support the targets **(To verify)**
- Establish a RAM policy, including the resolution of any conflict between 'safety' and 'availability'
- Identify the long term operation and maintenance constraints
- Identify any influence on RAM of the existing infrastructure constraints

Combined RAMS tasks comprise –

- Assessment of the adequacy of the information data and statistics used as input to tasks within this Phase **(To verify)**
- **Against the Deliverable from Phase 1 –** Assess the RAMS policy for compliance against the system requirements in phase 1 (ie the SAP, SSAP and RAMAP to include essential requirements outlined in phase 1) **(To verify)**
- Define system boundary, including -Interfaces with physical environment, technological systems and human beings
- Define the scope and the application conditions influencing the system, including - Constraints imposed by existing infrastructure, system operating and maintenance conditions, and logistic support considerations
- Define the scope of the hazard analysis, including –
  (1) Inherent hazards within the process to be controlled, and environmental and security hazards
  (2) Influence of external events and existing infrastructure constraints on RAMS
- Assess the adequacy of the methods, tools and techniques used within this phase **(To verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with assumptions and justifications

Phase 3 – Risk Analysis

General tasks comprise –

- Project related risk assessment

Safety tasks comprise –

- Perform a system hazard and safety risk analysis, identifying and prioritising all reasonably foreseeable hazards associated with the system in its application environment

- Identify sequence of events leading to potential accidents
- Evaluate the frequency of occurrence of each hazard
- Evaluate the likely severity of the consequences of each hazard
- Evaluate the risk to the system
- Determine and classify the acceptability of the risk associated with each identified hazard, having considered the risk in terms of any conflicts with availability and life cycle cost requirements
- Assess the risk acceptability classification **(To verify)**
- Assess the completeness of the risk assessment **(To verify)**
- Set up a hazard log for recording the risk analysis and the on-going risk management – to be updated whenever a change to an identified hazard occurs or new hazard is identified, throughout the life cycle
- Hazard log to be fully comprehensive, including all details from HAZOP worksheets
- Assess the suitability of the hazard log process for the system under consideration **(To verify)**
- Against the Deliverable from Phase 2 - Assess the hazard log management process for compliance against the system requirements in phase 2 (ie the hazard log management process to comply with the deliverables such as the SAP, SSAP and RAMAP outlined in phase 2) **(To verify)**
- Assess the adequacy of the information data and statistics used as input to tasks within this phase **(To verify)**
- Assess the adequacy of the methods, tools and techniques used within this phase **(To Verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with assumptions and justifications

(Note: There are no RAM tasks during this phase)
<u>Phase 4 – System Requirements</u>

General tasks comprise –

- Specify in further detail the system overall RAMS requirements
- Specify the environment in which the train will be operating
- Define the system demonstration and acceptance criteria for achieving compliance with the overall RAMS requirements
- Establish a validation management plan, including - Tests, analysis and demonstration to be carried out
- Establish the management, quality and organisational requirements
- Implement change control procedures (design)

Safety tasks comprise –

- Specify in further detail the system safety requirements overall
- Define the safety acceptance criteria overall
- Establish a safety management system over the defined safety related function requirements (ie to ensure that RAM studies do not affect agreed safety features)

RAM tasks comprise –

- Specify in further detail the system RAM requirements overall
- Define the RAM acceptance criteria overall
- Establish a RAM programme (ie more detailed than the RAMAP above) **(To verify – including the adequacy of the data sources included)**
- Establish a RAM management system
- Define the system RAM function requirements and structure

Combined RAMS tasks comprise –

- Assess the adequacy of information, data and statistics used as input to tasks within this phase **(To verify)**
- Amend the safety plan to ensure that all future tasks are consistent with the system's emergent RAM(S) requirements
- Assess the adequacy and completeness of the acceptance plan and validation plan **(To verify)**
- **Against the Deliverables from Phase 2 and Phase 3 –** Assess the system requirements against the SAP, SSAP and RAMAP (in particular the through life cycle costing), and the contents of the completed hazard log **(To verify)**
- Safety requirements to be reviewed against the safety targets, and any railway authority safety policies **(To verify)**
- RAM requirements to be reviewed against the RAM targets, and any railway authority RAM policies **(To verify)**
- Assess the adequacy of the methods, tools and techniques used within this phase **(To verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with assumptions and justifications

Phase 5 – Apportionment of System Requirements

General tasks comprise –

- Allocate functional requirements to designated sub-systems, components and external risk reduction facilities

Safety tasks comprise –

- Apportion systems safety requirements and targets
- Update system safety plans and validation plans (key aspects include the control of system interfaces where safety functionality may be compromised) **(To verify)**

RAM tasks comprise –

- Apportion system RAM requirements

Combined RAMS tasks comprise –

- Assessment of the adequacy of information, data and statistics used as input to tasks within this phase **(To verify)**
- Review the RAM programme
- **Against the Deliverable from Phase 4 –** Assess the RAMS apportionment, and the RAMS requirements for the system, sub-system, component and

external risk reduction facility, against the acceptance plans (including the through life cycle costing) **(To verify)**

- Assess the RAMS requirements for the system, sub-system, component and external risk reduction facilities to ensure they are traceable to the RAMS requirements for the system **(To verify)**
- Assess the RAMS requirements for the system, sub-system, component and external risk reduction facilities to ensure there completeness and consistency between functions **(To verify)**
- Assess the architecture for the total combination of designated sub-system, components and external risk reduction facilities to ensure it complies with the RAMS requirements for the total system **(To verify)**
- Assess the adequacy of the methods, tools and techniques used within this phase **(To verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with assumptions and justifications

Phase 6 – Design and Implementation

General tasks comprise –

- Design planning
- Design and development
- Design analysis and testing
- Design verification
- Implementation and validation
- Design of logistic support resources
- Realisation of design to meet RAMS requirements
- Establish plans in the context of RAMS for future life cycle tasks, including –
  (1) Manufacturing
  (2) Installation
  (3) Commissioning
  (4) Operation and maintenance procedures, including provision of safety related spare parts
  (5) Data acquisition and assessment during operations
- Assess consistency of the plan with RAMS requirements for the system **(To verify)**

Safety tasks comprise –

- Implementation of safety plan by review, analysis, testing and data assessment

RAM tasks comprise –

- Implementation of the RAM programme by review, analysis, testing and data assessment
- Programme control

Combined RAMS tasks comprise –

- Assessment of the adequacy of information, data and statistics used as input to tasks within this phase **(To verify)**

- Assess that sub-system and component designs comply with the RAMS requirements **(To verify)**
- Assess that sub-system and component realisations comply with the designs **(To verify)**
- Define and establish a manufacturing process capable of producing RAMS validated sub-systems and components
- Assess by analysis and test that the manufacturing arrangements produce RAMS validated sub-systems and components **(To verify)**
- Validation of sub-system and component realisation to ensure that the realisation complies with RAMS acceptance criteria for sub-systems and components, including through life cycle requirements **(To verify)**
- Ensure continued applicability of RAMS validation plans **(To verify)**
- Assess future life cycle activity plans are consistent with RAMS requirements for the system, including through life cycle costs **(To verify)**
- Assess the adequacy of the methods, tools and techniques used within this phase **(To verify)**
- Assess the competence of all personnel undertaking tasks within this phase **(To verify)**

The deliverables from the Phase to be documented, along with assumptions and justifications

Note:
The above linear sequentially ordered Phases are designed to provide a structure for planning, managing, controlling and monitoring all aspects of RAMS throughout the various design stages of the railway project (and Phases 1 to 14 throughout the whole life cycle of the project). This linear sequential ordering of the through life Phases, infers that the deliverables form one Phase become the inputs or the compliance standard for the next, or following, subsequent Phase(s). As a consequence, there are a number of specific verification issues to address at each sequential phase in the project

Validation issues are predominantly assessed during Phase 10 (ie System Acceptance), although of course some aspects must be validated as the design progresses

Section 11.0 IVV as a Combination of Auditing and Assessment

Verification and Validation can be considered as a combination of Auditing and Assessment, respectively, which can be identified and defined as two separate activities. However, although Auditing and Assessment are two separately identified activities, as defined below, there is a great deal of overlap and integration between the two

<u>Auditing</u>
Auditing – focuses on the engineering RAMS management processes and procedures, to ensure that they are appropriate and adequate, and that they are being followed. Where appropriate, the auditing will assist in identifying the root cause of any non-compliance in the established procedures and make appropriate recommendations to ensure future compliance. In particular –

- Auditing – is normally carried out against an approved and recognised standard of control (eg the Systems Assurance Plan, Systems Safety Assurance Plan and the RAM Assurance Plan etc, referred to above)
- Auditing – must be planned for and scheduled alongside the RAMS design activities and verification process
- Auditing – approval of control plans by so called 'triangle of control' – Primary Standard of Control (EN50126, Customer Technical Specification, SHE Legislation), Secondary Standard of Control - upper level (System Assurance Plan – SAP), Secondary Standard of Control - lower level (System Safety Assurance Plan - SSAP/ Reliability, Availability, Maintainability Assurance Plan - RAMAP)

Secondary Standards of Control – because the Secondary Standards of Control have been derived directly from the Primary Standards of Control – the plans SAP/SSAP/ RAMAP become the auditing compliance documents

Peripheral Management Standards – Secondary Standards of Control must be supported by Peripheral Management Standards, via a Safety Management System (above). Peripheral Management Standards comprise configuration management, design change management, systems interface and integration management, and approved documentation control, for example

General Management Procedures – all the above must be supported by General Management Procedures, again incorporated in the Safety Management System (above), and comprise the quality management system, and communications management, for example

- Auditing – a checklist is required which should comprise the essential elements of the above plans
- Auditing – involves: (1) Interviews with personnel, (2) Examination of project documentation and the organisation and level of control behind the written word of the documents, (3) Observations of processes and working practices, and (4) Demonstrations of traceable actions/ results/ decisions – back to their origin, such as the hazard identification process, and forward to the designed RAMS requirements (both requiring a study of the Hazard Log entries and Hazard management); and finally including the traceability of RAMS design project activities that implement the above planning requirements
- Auditing – requires documentary supporting evidence, signed off by a responsible person, that the planned activities have been carried out
- Auditing – non-compliances could be reported in categories in accordance with their severity (ie observations, reservations and concerns)

Assessment

Assessment – focuses on the product, to ensure that the risk associated with the system being developed has been reduced to a satisfactory level, to validate the results by two independent sources where possible, and where appropriate to assist in identifying the root cause of any non-conformance and make recommendations to restore confidence in affected areas. In particular –

- Assessment – in some respects is associated with a legal process (re: Risk Assessment, COSHH Assessment, Noise Assessment etc)

- Assessment – must be planned for and scheduled alongside the RAMS design activities and validation process
- Assessment – an aide memoir is required to ensure all planned aspects of assessment are covered
- Assessment – involves: (1) Critical review of the techniques, methods, controls and the results obtained, (2) Sample review of the accuracy of the RAMS design analysis carried out, (3) Comparison of the results obtained against the target values, and (4) Witnessing demonstrations to test, by computer or laboratory simulation, the validity of the theoretical RAMS design results obtained
- Assessment – requires documentary supporting evidence, signed off by a responsible senior project personnel, that the risk is ALARP on all major decisions leading to the critical RAMS design – prior to such decisions being incorporated by the justification described in the Safety Case
- Assessment – non-conformances could be reported in categories in accordance with their severity (ie observations, reservation and concerns)

The principles outlined above for auditing and assessment will satisfy the essential philosophy of EN50126 in terms of:

- Verifying: (1) the relevance and completeness of input data and statistics; (2) the various RAMS processes (ie HAZOP studies etc), including the training, competence, methodology and techniques against best practice (no indication in the Standard as to the depth of analysis required); (3) the management of identified hazards through to 'actioned' closure of the hazards in the Hazard Log; and (4) procedures and documentation produced against the Primary and Secondary Standards (upper and lower level), along with Peripheral Controls and General Management Procedures, and –
- Validating: (1) the RAMS results and the design against the target values, in order to –
- Establish: (1) the degree of compliance with the Standard's recommendations and planned arrangements; (2) that the planned procedures are implemented effectively; (3) that the procedures adopted are suitable to achieve the specified objectives and results, and (4) the results achieved will meet and conform to the targets values required

Notwithstanding the above, whilst auditing and assessment are somewhat akin to verification and validation, respectively, it must be said that 'verification' in particular is a through-life process. In other words, the appropriateness and adequacy of the deliverables from one phase become the inputs to a subsequent phase, and only by ensuring 'compliance' with the process and procedures at all phases can we achieve the correct validated results. This is in contrast to auditing which could be deemed a 'stand-alone' process, in making a judgement of a process against an approved procedure at a specific point in time

Section 12.0 Peer Review as an Aid to Auditing and Assessment

The Peer Review process can be seen as an adjunct to Auditing and Assessment (Verification and Validation), and is particularly important where domain knowledge has contributed to a subjective judgement as part of the RAMS design process, and so it is deemed essential to Peer Review the Method of Verification Control and

Observations made, as by definition, 'to verify' in this context refers to 'statements', 'procedures' and 'processes'. Where verification and validation is being carried out by an internal (independent) department, Peer Review by an independent external body is especially important. In particular –

- Peer Review process must be planned for and scheduled alongside the above Verification and Validation activities
- Peer Review the Method of Verification Control and Observations made with regards to compliance with the elements of the Secondary Standards of Control, in terms of – (1) Planning (via the appropriate documented procedures and a rolling programme of activities), (2) Controlling (via evidence of working to the procedures identified above and the RAMS programme), (3) Managing (via evidence of a Safety Management System of Control), (4) Monitoring (ie the effectiveness of management control over the process), (5) 'Transparency' (ie traceability, to allow audit trails to take place on the identification of RAMS decisions and activities), and (6) Justification (via a Safety Case to justify the results obtained)
- Peer Review the Method of Verification Control and Observations made regarding – (1) Relevance and Completeness of Input Data (qualitative and quantitative), and (2) Process, Techniques and Methods for Best Practice and Management Control
- Peer Review the Verification Control Process and Observations made regarding – Tracing back over the hazard management control to the origins of the data, stemming from hazard closure results identified in the Hazard Log – via input data, HAZOP study worksheets, evidence of control measures, actions etc (ie traceability of information)
- Peer Review the Method of Verification Control and Observations made regarding – Sampling the checks on design decisions to trace the controls over the design process and decisions made
- Peer Review the Method of Validation Control and Observations made regarding – Management and Actions taken over the RAMS results, relative to the target values

Section 13.0 Conflict of Safety Cost and Availability Economics

Safety and RAM studies are normally carried out in parallel, along side each other, during the preliminary and detailed design phases. The reason being is that, 'safety' is the avoidance of accidents/ incidents and as such has a cost dimension attached to it, but on the other hand RAM (particularly the 'availability' element) is economically driven in the sense that the overall life cycle costs will be reduced by the increased operational availability of the railway system. Therefore, it will be seen, that there could be an element of potential conflict between the increased cost of ensuring that the railway system is safe (Including any system outage time during which safety checks are being carried out), and the overall reduction in the life cycle costs of operation by making the railway system more available at all times. So it follows that if a RAM study were to be undertaken separately and at a later stage to the safety evaluation, then any design decision made in the interests of the availability element of RAM, could jeopardise or compromise earlier design decisions made with regards to operational safety

Quite often conflict will inevitably arise when reviewing the 'availability' element of RAM. As a consequence an optimum balance must be achieved between the safety, reliability and the reduced risk of operating the railway system on the one hand and the economic issues of reliability, availability, maintainability and supportability associated with the customer's technical specification regarding life cycle costs of operating the system. This sometimes leads to a 'trade-off' between safety and RAM during the design phase. However, having said that, the design integrity and operational safety must not be compromised. In order to ensure that critical safety elements of the design are not compromised, a range of 'Safety Integrity Levels' (referred to as SILs) are established, depending upon the criticality of various elements and sub-systems incorporated in the design

Section 14.0 Lessons Learnt

Based upon the author's experience in the role of an Independent Verification and Validation Consultant, there are a number of key issues that must be addressed in order that the process is effective in verifying the requirements and deliverables in each phase, and that ultimately the design corresponds with the customer's requirements. In particular, reference is made to the following, which is not in any specific order of importance –

- There is sometimes difficulty in correlating the design stages with the so-called linear design phases of EN50126, and so there can be difficulty in establishing whether the company has addressed all the elements of EN50126. As such the RAMS programme needs to be accurately correlated with the phases of EN50126, otherwise there could be overlapping of the elements in the phases of EN50126, or more importantly, omissions
- Plans are sometimes not adhered to (treated as an academic exercise)
- Unofficial documents are sometimes presented for Preliminary Design HAZOP sessions. Each stage in the design process must be officially signed off
- Reference system data on accidents/ incidents is sometimes not made available for political reasons
- Claims are sometimes made to reduce the 'risk' by undocumented proposed control measures
- There can be a cultural issue with the designer/ manufacturer – adopting a 'bottom-up' approach, and customer adopting a 'top-down' approach. Bottom-up: reliability built into product at manufacturing stage with extensive QC; Top-down: systems integration concept with reliability inherent in design and filtered down through the product (reference Gestalt behavioural learning theory).
- There is sometimes no evidence of cost-conflict philosophy, addressing any conflict between safety and the prevention of accidents, and 'availability' which is primarily cost driven
- Human factors/ ergonomics is sometimes not being addressed early enough in Preliminary Design, no human factors engineering plans, cultural problems with the concept of human error (too much reliance on future training and procedures as control measures at Preliminary Design) ie. pass the problem onto the operator rather than solve the issue during design.

- Life cycle costing is sometimes not addressed at Preliminary Design – even though maintainability and operational strategies have been addressed at this stage
- Safety and RAM is sometimes treated separately which can lead to design conflict (safety – prevention of accidents, availability – cost driven). No decision policy or protocol has been established if conflict does arise
- There is sometimes very little evidence of design change management, as a part of configuration management control
- There is sometimes no independent systems integrator to address sub-system interfaces and systems integration. This is particularly important and much emphasis is placed upon this element as it may have cost and timescale implications
- Software systems are sometimes developed without an independent software assessor to oversee and assess the SIL requirements (Cost of an unnecessary increase in the SIL requirement for a function increases exponentially)
- Too much emphasis is sometimes placed upon software control by mechanical design engineers
- The designers sometimes have no Verification and Validation Plans, or Safety Auditing Plans, developed as part of a Safety Management System
- There is sometimes no effective Safety Management System. This is extremely important in the context of verification and validation
- There is sometimes ineffective project management which means that RAMS issues are not being fully integrated into the design process

Section 15.0 Conclusions

The essential message to be taken on board from the interpretation of the Standard is:

- The elements of EN50126 is must be managed and controlled by a Safety Management System
- The Safety Management System must be integrated with the existing Management Structure and Procedures
- Only then can we have effective Project Management and Compliance with EN50126

Section 16.0 About PMSC Limited

Dr. Eric Long is an associate of PM Safety Consultants, which is a specialist Systems Assurance company, offering Systems Safety advice and Reliability, Availability and Maintainability assurance support to a range of industries worldwide. Our web site is located at www.pmsafety.com