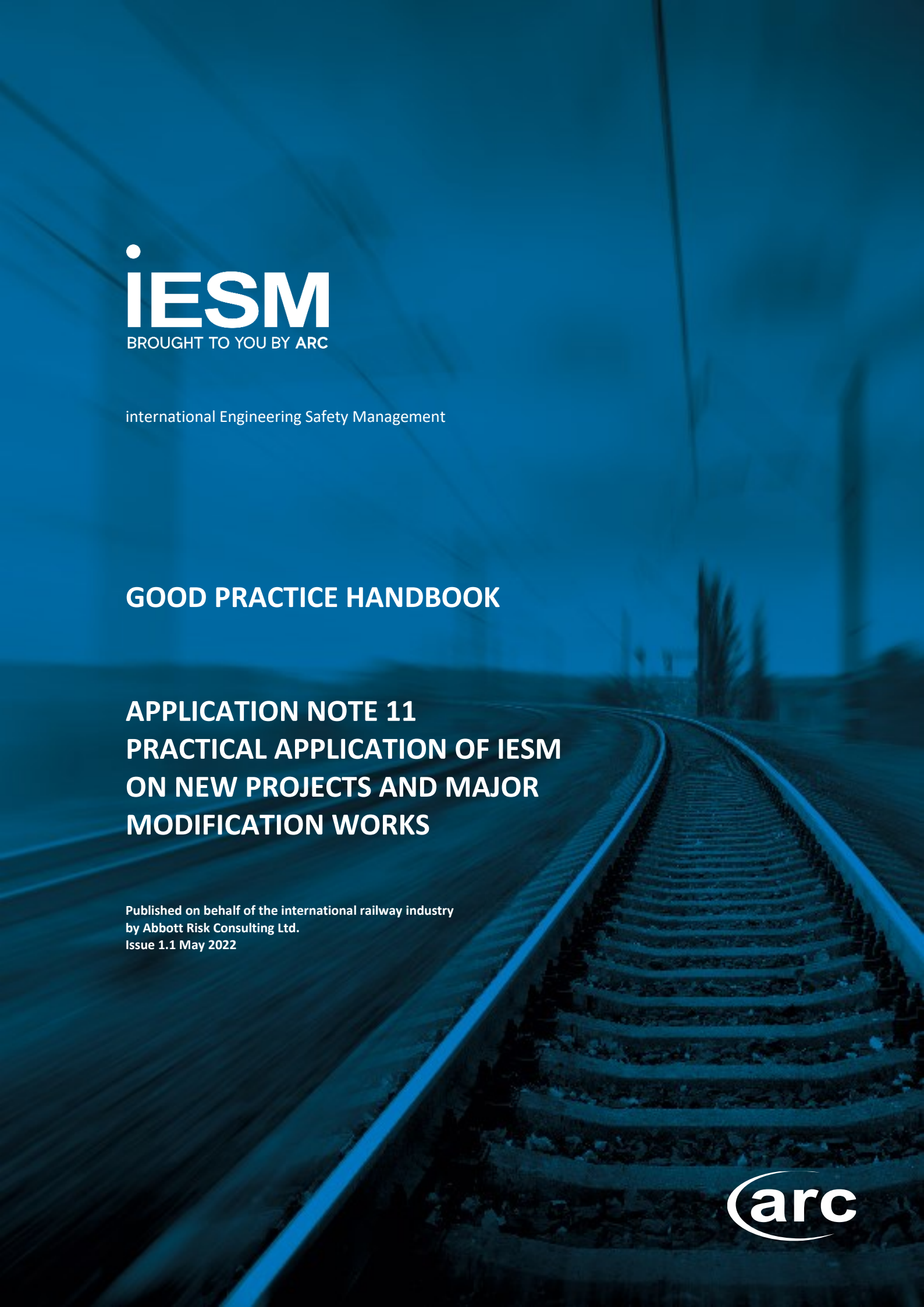

IESM
BROUGHT TO YOU BY ARC

international Engineering Safety Management

GOOD PRACTICE HANDBOOK

APPLICATION NOTE 11
PRACTICAL APPLICATION OF IESM ON NEW PROJECTS AND MAJOR MODIFICATION WORKS

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.1 May 2022

arc

CONTENTS

Issue 1.1

DISCLAIMER

Abbott Risk Consulting Limited (ARC) 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 handbook has been written with help from the people listed below.

- Mike Castles
- Greg Newman
- Paul Cheeseman
- Bruce Elliot
- Katherine Eastaughffe
- Gab Parris
- Peter Sheppard
- Gareth Topham

These people worked for the organizations listed below.

- Abbott Risk Consulting Ltd.
- Acmena
- Ricardo Rail
- Technical Programme Delivery Group
- Rio Tinto
- WSP

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

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 belongs in the second layer. The current Volume 2 provides guidance on implementing the generic ESM process presented in Volume 1 on projects. At the time of writing, this AN contains the content of a second Volume 2 providing guidance on implementing the generic ESM process presented in Volume 1 for maintenance. It is hoped to republish it in that form in due course.

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 11. It supports the main body of the handbook by providing guidance and checklists that may be used when carrying out some of the ESM tasks in a maintenance context.

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.

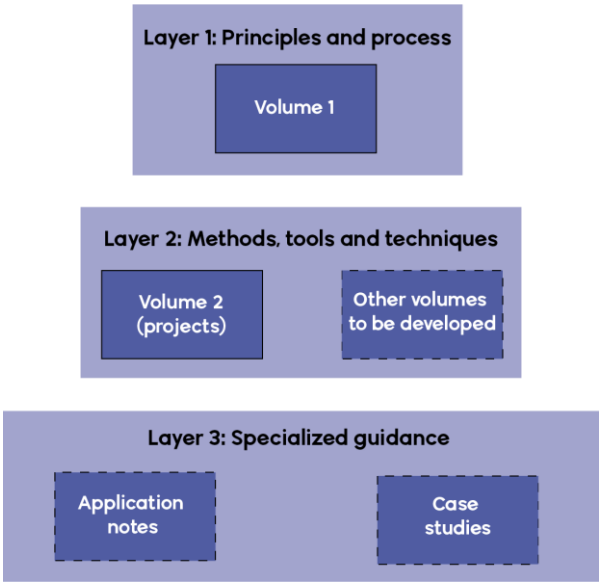

Figure 1 The Structure of iESM Guidance

2 BACKGROUND

2.1 Purpose

This AN expands on the guidance provided in Projects Volume 2 of the iESM guidance. It is written for people who use their judgment to take or review decisions that affect railway systems. If you only take or review decisions within a framework of established procedures, you may not find it necessary to read this guidance.

If you are managing a multi-disciplinary project the entire AN may be helpful.

Guidance is provided on how the principles may be achieved. The guidance should be interpreted to meet the needs of straightforward projects or ones that had been delivered many times. In general, it should be obvious whether this is true or not, but it may rely on professional judgement by responsible experts who are familiar with good practice in the field.

This AN provides guidance on the working inter-relationship between engineering safety management, systems engineering and project management disciplines from the point of view of the ESM practitioner. It should be read in conjunction with iESM Volume 2 which provides extensive information, background and guidance on the various methods, tools and techniques.

2.2 Systems, sub-systems, projects and environments

A railway is a system, that is, a collection of assets, people and procedures that are intended to work together to accomplish some function. There are smaller systems within railways. These include signalling systems, track systems, stations, depots and trains. The whole railway is a hierarchy of systems and sub-systems, sometimes called a “system of systems”.

Except for projects that deliver only paper, such as feasibility studies, railway projects exist to make changes to the railway. These changes can always be characterised in terms of creating a new railway system or changing an existing one.

Projects deliver or contribute to the delivery of new and changed railway systems. In the rest of this handbook, unless stated otherwise, the word “system” means the railway system that is being delivered or changed. The environment of a system means the parts of the rest of the world that the delivered system interacts with. The environment of a railway system will include neighbouring parts of the railway but usually other things outside the railway as well; for example, the environment of a level (grade) crossing includes road vehicles and their drivers.

2.3 Multi-Disciplinary Projects

Excellent discipline engineering and project management are necessary to deliver successful railway systems but are not sufficient to ensure success of a project. Many of the criteria which stakeholders ultimately use to measure success are technical but are not contained within any one discipline, and normally require all disciplines to be successfully integrated to achieve the intended outcome.

Consider an upgrade to an electrified railway which is designed to reduce journey times for example. Journey times are a function of rolling stock performance, electrification power capacity, permanent way and signalling as well as timetabling considerations. Delivering reduced journey times reliably and cost-effectively requires effective co-ordination of all these disciplines as well as other specialisms (for example, simulation). Properties like journey time that can be measured only for the railway as a whole, not for any part of it, are called emergent properties of the delivered system.

It is a rather cryptic name for a straightforward idea and a bit misleading – emergent might suggest that no action should be taken to influence the value of these properties because they will “just happen”. On the contrary, they must be addressed by design to prevent them emerging with unacceptable values.

2.4 The management of engineering safety

Safety is another emergent property of the railway. In principle, Engineering Safety Management (ESM) is a branch of System Engineering (sometimes called Systems Integration). In practice, safety management is subject to specific legislation and regulation which prescribes certain processes that are not generally appropriate for managing other emergent properties. However, activities to manage safety and non-safety emergent properties interact because:

- Some non-safety emergent properties are aligned with safety and can be pursued together. All other things being equal, a more reliable railway is a lower risk railway, for example.
- Some non-safety emergent properties may be in conflict with safety and these conflicts must be resolved. All other things being equal, a faster railway is a higher risk railway, for example. Because the resolution of such conflicts is generally regulated in law (with safety required to be paramount), they are normally resolved by Systems Engineering and Engineering Safety Management processes.

2.5 Safety management within a project context

To assist in contextualising the guidance in this AN, we have considered the interaction of engineering safety management with the disciplines of project management, systems engineering, and the role of Independent Professional Review similar in concept to an extension and expansion of Table 1 in EN50126 [2]. As we proceed through the various stages of the project lifecycle, we will contextualise the activities of engineering safety management with those of these other disciplines so that all parties gain a clearer and broader understanding of the inter-relatedness of these roles.

It is stressed that there is no single “right” way to approach this, but experience shows that there are many less successful ways.

3 SYSTEM LIFECYCLE

3.1 Overview

Any railway project (for example, a new train, a new signalling system, major civil engineering works) can be considered to evolve through phases such as:

- **Project / System Concept** – Project planning takes on a more complex nature when it comes to more than just the development of a single standalone product, and in particular, when changes/upgrades/renewals are being made to an operating railway. In these situations, many more real-world constraints must be managed such as interfacing or interrelated projects, progressive releases of incremental functionality or geographic coverage, etc., as well as the need to schedule (and ensure the safety of) site testing (even if this is done in non-traffic hours or on an isolated section of the railway). If these are not fully recognised and communicated appropriately in a document, then operational safety may be compromised. In this respect, the planning of safety assurance activities should reflect the planning of the overall project delivery.
- **Systems Specification & Requirements** - All activities that culminate in Requirements Definition – the agreement on what is to be achieved. Typically, these will involve clarifying what the needs are; outlining one or more potential solutions; checking whether these solutions are feasible; selecting one potential solution to proceed with and describing the contractual framework within which the solution will be implemented. The output will be a set of documents defining the needs, the proposed solution and sometimes the contractual framework. The Requirements Definition follows and is the definition of a precise set of requirements against which the project's final success can be measured. The output will be a requirements baseline – a set of documents specifying these requirements. The output may also include the necessary contract strategy to carry out the work. As part of the devolution process, the system concept and objectives will be devolved and/or apportioned into requirements for each and any (sub)system required to meet the scope and objectives. Traceability between objectives/scope/concept and the defined requirements is essential and an early step in the validation process will be to demonstrate that the aggregate of system/subsystem requirements will deliver the project scope/concept/objectives.
- **Design** - All the design activities that need to be carried out to produce the delivered system that will meet the defined requirements. The Design phase results in a baseline – a set of documents and drawings for the chosen design. The majority of the work to obtain safety approval should be carried out in this phase.
- **Implementation / Integration** - All activities that are involved in realising the design, including all construction works as well as the integration of electrical, electronic and mechanical sub-systems and delivering software and application data. The output will be a physical system baseline and an as-built documentation set.
- **System Validation & Acceptance** - All activities required to bring the delivered system into full service, including obtaining final safety approval, testing and commissioning for signalling and trial running for trains. This phase means very different things to different disciplines. It may be very short for civil works as the necessary approvals are typically obtained during implementation. This phase sees the culmination of the design and implementation verification and validation activities.
- **Operations and Maintenance** - All activities involved with the normal operation of the delivered system. Note that this means very different things to different disciplines. It may include continuing adaptation of the delivered system, particularly for rolling stock. This includes replacement of components and sub-systems within the delivered system. This phase ends when the delivered system is removed from service.
- **Decommissioning and Disposal** - All activities involved in removing both a previously delivered but now obsolete system, and the newly delivered system once it is obsolete, from the railway. For example, demolition of civil works and removing or making safe trackside cabling.

This sequence of phases is called the system lifecycle. Note: this lifecycle is derived from the generic lifecycle set out in volume 2 of the iESM guidance [1].

Verification takes place at each lifecycle phase and hence is not a specific lifecycle phase of its own. It consists primary of the following:

- Auditing the implementation of planned activities at each lifecycle phase
- Ensuring traceability of requirements at the end of each phase from the end of the Project/System Concept phase through to the beginning of the Operations and Maintenance phase

We acknowledge that many readers may be familiar with the CENELEC series of standards (EN50126 [2], EN50128 [3], and EN50129 [4]). Where it may assist understanding of this AN, we have included a comparison between the above lifecycle phases and those defined in EN50126 [2].

3.2 Limitations and application of the system lifecycle

The system lifecycle is an idealisation – in real projects different phases may be executed in parallel and there will be iteration. Moreover, the sequence may well be branched.

Although the system lifecycle is an idealisation, it is possible to use it as a reference point and to refer real projects back to this lifecycle. If the project scope excludes a phase and there may be deficiencies in the way in which it has been or is being done, this may introduce risk to the project. It is sensible to weigh up all the commercial and technical considerations before taking an informed decision whether to accept, reject or challenge the project scope.

3.3 Cross-lifecycle activities

Successful delivery of each phase in the system lifecycle relies upon support from a number of System Engineering activities which run throughout the project. We refer to these as cross-lifecycle activities.

4 ESM IN A PROGRAM CONTEXT

4.1 Introduction

This section is provided to put into perspective the broader context where ESM is likely to be beneficial e.g. a large program. Unless the broad context is understood, the benefits of ESM may not be fully realised.

This section discusses a wide range of issues that are relevant to the application of ESM to real projects.

4.2 Safety Planning

All ESM activities should be planned before they are carried out. The project should produce a System Safety Plan (SSP) or similar document which complies with the guidance in [1] clause 6.2. The project should therefore follow these steps in planning ESM activities:

- Identify the relationship between the proposed work and the system lifecycle described in Section 6. Also map the systems lifecycle to their specific project's lifecycle (the major phases of the project);
- Assess the degree of complexity and novelty associated with the proposed work and plan activities in order to focus necessary special attention to these complex and/or novel areas;
- Establish the safety objectives of the project;
- Specify how the project will address each of the cross-lifecycle System Engineering activities and the phase-based System Engineering principles contained in [5] which are relevant to the work in a way which is consistent with the complexity and novelty associated with the project.

Competence of the project team is a critical factor in the success of the project [1] clause 21, and it should be considered carefully at the planning stage.

4.3 Necessary Constituents for Delivery Success

The following general management framework, resources and controls are a prerequisite to a successful project:

- **Strong Programme & Project Management** - (using sound project management applications, processes & tools). This includes precise scope definition, programming of activities and reviewing progress against realistic schedules with the necessary logical connections. Having a common, combined project program showing how engineering safety management activities link with other activities from system engineering, is essential for the effective co-ordination of safety.
- **Effective System Integration processes** – using proven techniques that are appropriate to the project concerned and fully integrated into core project activities.
- **Experienced Teams** – with the necessary competence and experience covering the System Integration processes and the relevant discipline engineering.
- **Effective Risk Control/Issues Resolution** – Processes for identifying, monitoring and resolving the highest risk aspects of delivery. The engineering and project management risks and processes should be integrated and reporting a consistent message.
- **Effective Communications** – The general arrangements, risks and processes including System Engineering activities need to be communicated and understood by the project, client team and supply chain organisations to the extent necessary to support successful delivery. See [1] clause 22 and 23 for detailed guidance on this issue.
- **Effective Monitoring (KPI, etc)** – Key project processes including the System Engineering processes should be monitored placing appropriate emphasis on the quality of the output as well as time and cost.

The next section highlights real-world problems and explains how the items above may be addressed.

4.4 Potential real-life problems

Although the essential constituents for successful projects would be widely recognised, they are not enjoyed by all projects in practice and the following problems are often encountered.

- **Requirements not well defined, but the programme must be met** – Even though the need for clear scope and requirements are understood, the time to achieve the clarity is often not available and senior management often demand signs of physical progress. This failure is one of the earliest causes of the project not achieving its purpose and potentially experiencing serious time and cost overruns or compromised safety.
- **Management arrangements not shaped to the specific challenges of the project** – Generic arrangements are often provided for projects without the essential tailoring of them to the specific needs, technology and challenges of the project. At best this is inefficient; at worst it leads to delivering shortfalls, schedule slippage and cost overruns.
- **Not integrated in practice** – Even where project team members share common objectives, their priorities and focus are often different resulting in:
    - Project Managers and the project team not being aligned
    - Different objectives, challenges and priorities in different areas
    - Programme risk management not tightly linked to engineering technical risks and critical issues
    - Poor communications - "too much talking, not enough listening" or failure to adequately or accurately describe and record critical issues
- **Quality of the staff and relevance of their skills often mismatched to the programme challenges** – All too often staff are selected on inappropriate criteria such as availability, hourly cost, partial skill sets rather than securing the staff with appropriate levels of experience and competence to address the project and technology challenges. This can result in compromised safety, failure to achieve system/asset acceptance, and cost/time overruns.
- **Key stakeholder & supplier relationships not mature or inappropriate contractual relationships** – Whereas stakeholders and suppliers may have aligned objectives when things are going well, problems can lead to conflict and blame responses rather than resolving problems critical to delivery.
- **Processes not mature** – System safety and project management processes, especially System Engineering may not be sufficiently mature for effective delivery. This is particularly true for new companies such as collaborations between two or more companies where new management systems are developed, and new areas of technology are used. This can result in compromised safety, poor RAM performance, inability to meet system/asset performance targets, failure to achieve system/asset acceptance, and cost/time overruns.
- **Program not correct or not adhered to** – Sometimes the design or other activities race ahead of the engineering safety management activities (most often due to schedule pressures). This generally results in the engineering safety management role lagging far behind the progress of what may be an already approved design, only to identify deficiencies in that design which project management is reluctant to have corrected due to these cost and schedule pressures. It can also lead to contracts being awarded before the project requirements are fully understood which results in, at best, project delays, cost overruns, or a poorly reputed project.
- **Lack of a common understanding of engineering safety management activities** – Sometimes, the engineering safety management activities are seen as a separate discipline, isolated from what is otherwise regarded as the main engineering activities. This can result in compromised safety, failure to achieve system/asset acceptance.
- **The inaccurate allocation of Safety Integrity Levels or a misunderstanding of the "SIL 0" or "Basic Integrity"**– Sometimes functions allocated SIL 0 (or "No SIL") are not given the attention they deserve in relation to the dependability of the delivered and commissioned system
- **Inappropriate use of Commercial Off The Shelf (COTS) equipment** – The use of COTS equipment can have benefits in relation to safety, project cost and time. However, COTS equipment is not tailored to a specific application and hence it must be selected carefully on the basis of its environmental performance, its inherent functionality versus its required functionality, and its safety justification. Thus, the evaluation, selection and cross-acceptance of safety justification must be carefully undertaken noting that as soon as modifications to the COTS are required for any reason, it is no longer COTS but

is Modified COTS. Any COTS (or modified COTS) incorporated into the delivered system must be subjected to the safety assurance processes indicated in this AN11 to the extent of the safety-reliance placed upon it. Failure to do so can result in compromised safety or failure to achieve system/asset acceptance.

- **Inconsistent team membership** – Work is only done by people and the flow of people into and out of the project results in gaps in knowledge and familiarity with the details of the project (not everything can be documented). Team reorganisations can have the same effect. This flow (or churn) can negatively impact the integrity and quality of deliverables.

These fundamental problems, if left unchecked, can lead to:

- Requirements change
- Key process breakdown
- Emerging properties becoming out of control
- Breakdown of client/project relationships
- Loss of detailed project knowledge
- 'Silo' mentality where people do not understand or identify interdependencies with other teams and manage these interdependencies
- Bad publicity
- Inability to achieve, or to demonstrate the achievement of, safety targets and objectives or a dependable system

Sections 5 and 6 identify the arrangements necessary to avoid these problems.

4.5 Safety Integrity

The latest CENELEC standards EN50126 [2] introduce a concept of "basic integrity" which is an additional level of integrity below that of SIL1 but still having some reliance upon them for safety. EN50128 [3] refers to these as SIL 0 functions. In the past projects with functionality less demanding than SIL1 were treated as non-safety related. Experience has shown that there are functions that, although they do not warrant the cost or complexity of the SIL-related techniques specified in the standards, nevertheless need to work dependably. It should be noted that the justification for the integrity (dependability) of a SIL 0 function may be similar to that required for any low SIL-rated function.

The following requirements apply at system level where the basic integrity function is integrated:

a. For life-cycle phases 1 to 4 before being classified with the attribute of "basic integrity", the function shall be evaluated in the risk analysis process and results be traced in the hazard log.
b. At the life-cycle phase 6 "system design" adequate fault management measures shall be provided, such as diagnostics, maintenance, operator training and adequate procedures.
c. At the life-cycle phase 8 "integration":
    - any (non-trivial) assumptions made in the process of allocation of safety requirements shall be traced as safety-related application conditions (SRAC);
    - the function shall be included in the System Validation test (including impact analysis on other SIL functions);
    - non-intrusiveness (i.e. absence of retroactive (undesired) effects, that is the function does not affect other safety-related functions) shall be demonstrated.
d. At the life-cycle phase 9 "validation" the safety case shall address the safety-related function.
e. At the life-cycle phase 11 "operational" a follow-up shall ensure the basic integrity function remains in operation (maintenance inspections and/or failure analysis (i.e. Data Recording, Analysis, and Corrective Action System (DRACAS)) in order to check that the random failure target is not exceeded).

4.6 Safety Cases on a Project

A final Specific Application Safety Case will be required for every version of the delivered system placed into operation. Note that this may relate to an increasing set of functionalities or an expanding geographic area of coverage being progressively delivered. For complex projects, the Specific Application Safety Case may need to be supported by one of more of a Generic Application Safety Case and/or a Generic Product Safety Case. A safety case or safety justification statement may also be advisable for each stage of on-site testing (be it dynamic testing of rolling stock or cut-over of infrastructure etc.) if risks are considered to warrant one. What can be less clear is how this may relate to the various works of a project, (the scope of which may extend from the lowest levels of software or hardware development/modification to in-service operation of the delivered system), and the need for, and relationship between, other safety cases.

iESM [1] section 13.2.8, EN50126 [2] clause 8, and EN50129 [4] clause 7 all provide guidance on the various safety cases which may be relevant in any particular project. Depending on the scope of the project, any combination of one or more generic product safety cases, generic application safety cases, and/or specific application safety cases may be required. Figure 2 below, from EN50129 [4], indicates a possible relationship.

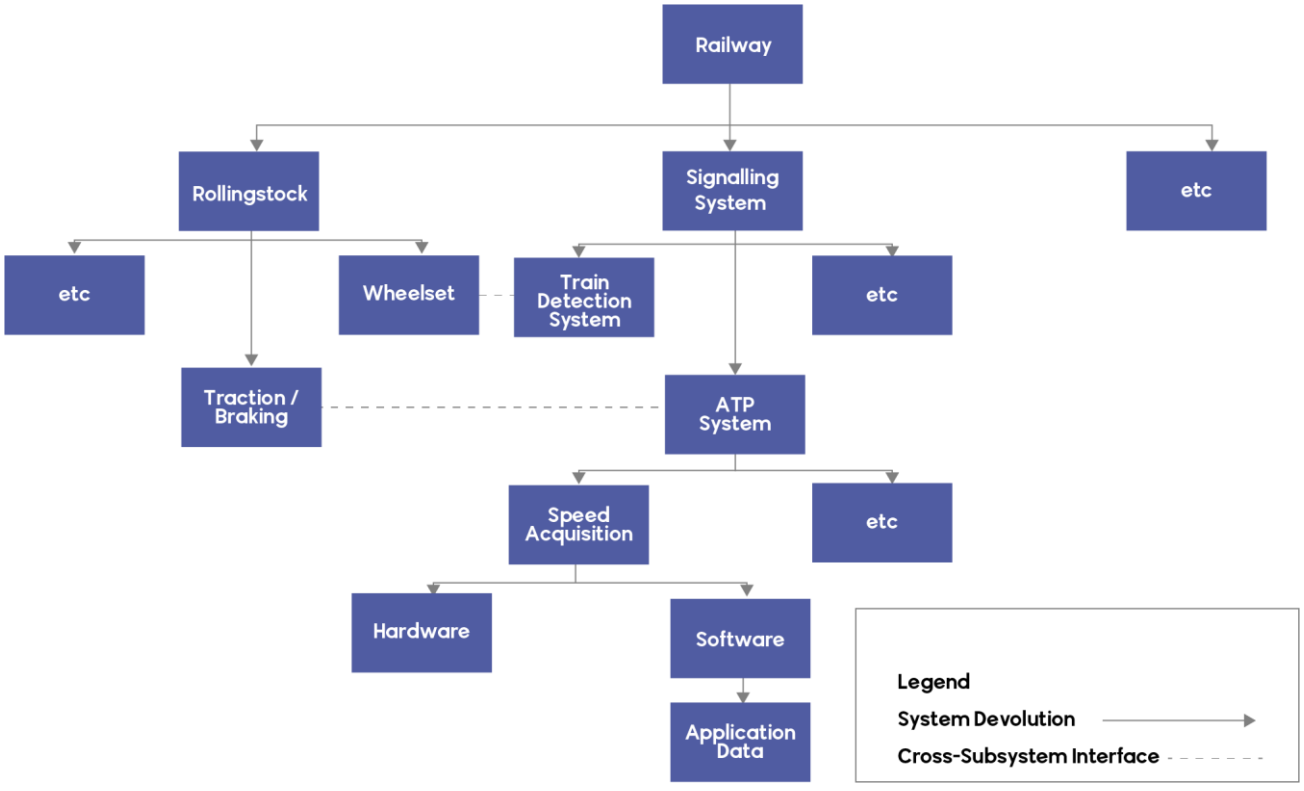

Figure 1 Example Safety Case Relationship for a Signalling System

Note that the approval of a safety case may be used as a necessary (but insufficient) condition to demonstrate successful progressive integration of the delivered system. The integration path can be linked to the safety cases from the integration of software and hardware into a generic product (generic product safety case), through the integration of products into generic sub-systems and generic systems (generic application safety case) to the final integration of the delivered system into its specific operating target environment (specific application safety case). The concept is presented in the table below.

Level of integration	Signalling Examples	Civil Engineering Examples	Mechanical Engineering Example	Relevant safety case
Software integrated (where applicable) with hardware (electrical, electronic and mechanical) items to form a generic product	Electronic track circuit, Point machine	NA	NA	Generic Product Safety Case
Generic products integrated to form a generic sub-system	Track circuit, point machine, lineside signals etc. to form a generic signalling system	Load bearing arches adequately supported by foundation structures or piling	A generic fuel pump integrated into a motor package	Generic Application Safety Case
Generic products and/or generic sub-systems integrated to form a generic system	Train carried ATP/ATO, lineside Radio Block Centre, Vital Signalling Server etc., integrated to form a generic ETCS system	Double glazing units integrated into a rainproof wall	A motor package adequately isolated from the effect of shock/vibration in the vehicle chassis	Generic Application Safety Case
A generic system, specifically commissioned with site-specific application data and architectural configuration integrated into a specific operating target environment and interfaces	Train detection device, points machine, Train carried ATP/ATO, lineside Radio Block Centre, Vital Signalling Server etc., integrated to form the ETCS on a specific target piece of railway.	A conventional bridge design integrated with foundations or piling designed for the local geotechnical conditions	A standard car design with tyres and engine management configurations chosen for arctic operational conditions	Specific Application Safety Case

The key issue is that the chosen safety case relationships should be developed to align with the scope and staging/milestones of the project and the delivered system's architecture. Any misalignment may result in gaps (incompleteness) in the overall safety justification, or a completed safety justification not being available when needed for a particular project milestone such as introduction into service.

4.7 Management of Multiple Organisations

Many railway projects involve multiple organisations operating in a supplier hierarchy to produce and commission a delivered system. It is almost certain that each organisation will have its own particular way of doing things, but the more these processes differ, the more the opportunity for safety to "slip between the gaps". This tendency can be reduced by adopting the following strategies: -

- Planning documents, particularly System Safety Plans, Project Management Plans, Verification and Validation Plans, and Configuration Management Plans, should be written in a hierarchy so that higher level plans place specific requirements for alignment on lower level plans and lower level plans align with and feed into higher level plans
- There should be a single strategy for the development of Safety Cases across the various levels of suppliers with this strategy being specified in the highest level System Safety Plan with all lower level System Safety Plans reflecting in detail, and delivering upon, that top level strategy.
- Safety Cases should be developed at each appropriate level of the supply chain to implement the safety case strategy.
- There should be a single strategy for the management of Hazard Logs (including SRACs) across the various levels of suppliers with this strategy being specified in the highest level System Safety Plan, and all lower level System Safety Plans reflecting in detail, and delivering upon, that top level strategy.
- There should be a single strategy for the implementation of the DRACAS across the various levels of suppliers with this strategy being specified in the highest-level System Safety Plan, and all lower level System Safety Plans reflecting in detail, and delivering upon, that top level strategy.
- The overall program (the amalgamation of each contributing project's Gantt chart) should be constructed as a single entity "whole" with strongly defined stage gates.
- Any contracts or sub-contracts utilised to deliver the project should constructed according to an overall contracting and procurement strategy. Incorporation of the defined stage gates (see above bullet point) into the contracts is essential.

See iESM [1] sections 16, 22 and 23 for further guidance.

5 SYSTEM INTEGRATION

Systems Integration is a subset activity of System Engineering and is described and defined in IEC 15288 [5] at section 6.4.8. While some may view systems integration as being putting systems to work together in the factory and on the railway, {5} clause 6.4.8.3 item b) applies to EVERY element of the final system, from software and application data, to electronic and mechanical hardware up to and including the final new configuration of the operating railway.

5.1 System-of-Systems Concept

All "systems" are comprised of one or more component elements or sub-systems (which in turn may be comprised of one of more elements). A signalling system may comprise an interlocking, train detection/location, a points machine, and a means of conveying a safe movement authority to a train and potentially for enforcing such safe movement authority, etc. An item of rolling stock may comprise a body, bogies, a braking system and a propulsion system, etc.

This approach has many advantages in terms of re-use of existing components, configurability, parallel development, etc., however as soon as decomposition into sub-systems/elements begins, so too is an interface defined, which represents a point where integration of these sub-system/elements into the whole system of interest is required. This system-of-systems approach is further developed in IEC15288 [5] from which the following figure is taken.

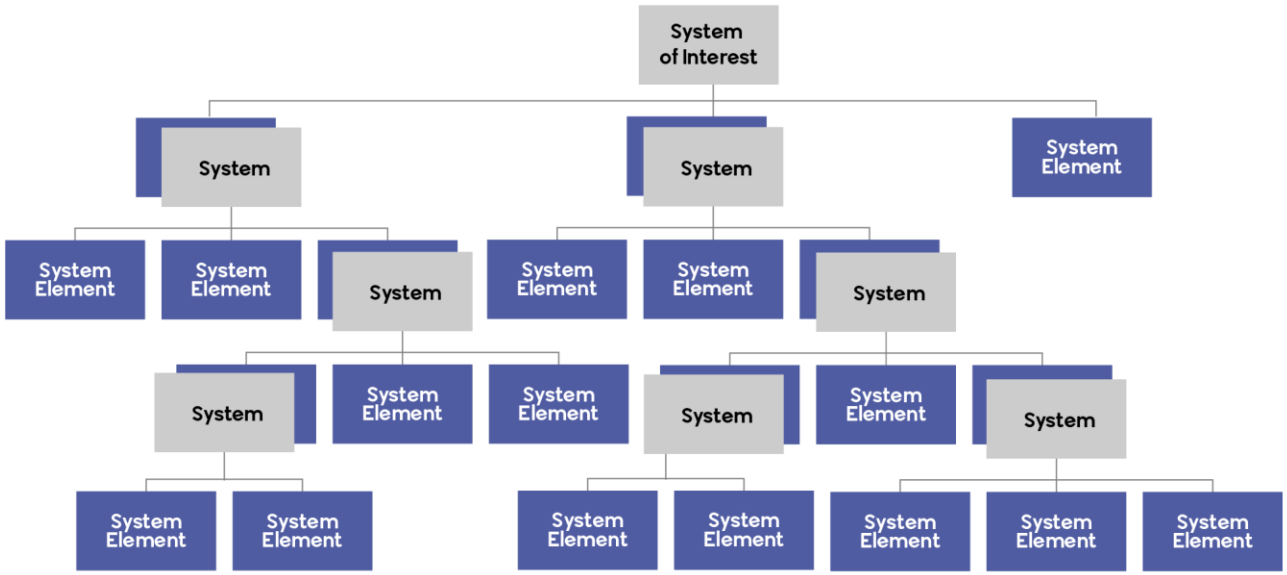

Figure 2 "System-of-Systems" IEC 15288

We introduce this concept of a system-of-systems being comprised of various elements or subsystems as it has parallels in engineering safety management as the hierarchy of systems portrayed in iESM [1] and the iESM training course.

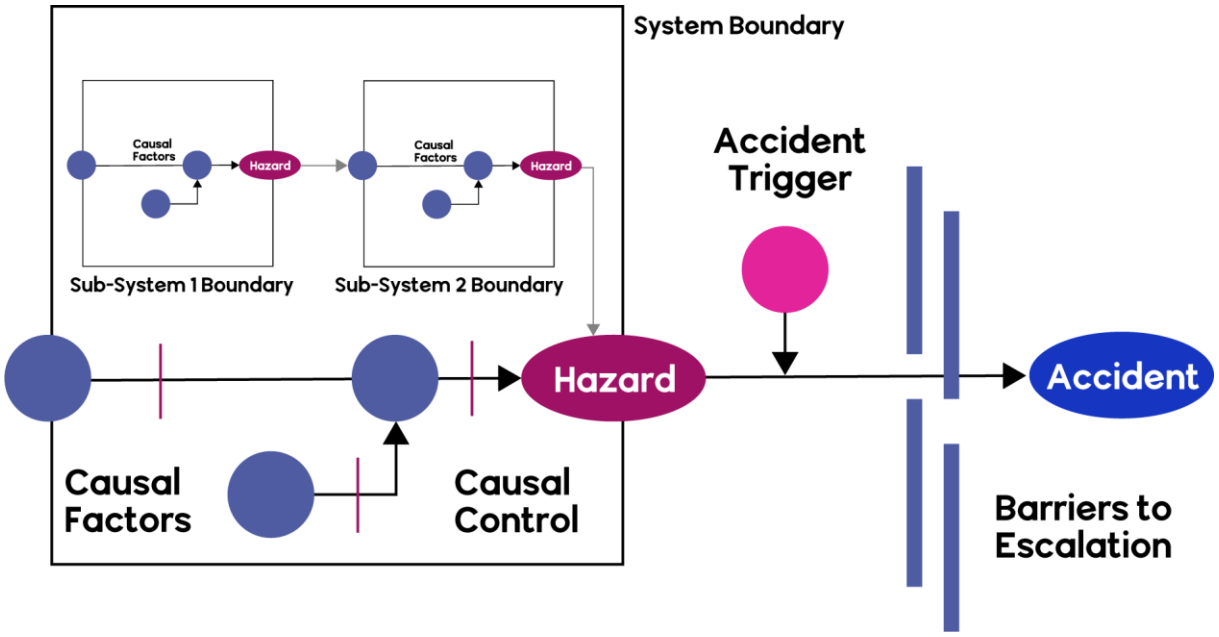

Figure 3 Hierarchy of Systems iESM Volume 2

This concept can be extended into the hierarchy indicated below in Figure 5 where the highest level "system" (here shown as the railway) is devolved down to the lowest level constituent components. In this example we have chosen to follow the devolution from the railway down to the signalling system, but the concept applies equally well to rolling stock, traction power systems, etc.

The key point to note here is that each time we take a step in splitting a system into its constituent parts, we determine an interface, either directly "down" the chain of devolution, or "across". In Figure 5 below, this is represented as rolling stock. Each step represents an interface (which needs its own interface specification, interface design, and interface hazards, etc.), and at which (once we start to develop our system by re-integration) integration takes place until we reach our integrated top-level system as a whole.

As Figure 4 above implies, a sub-system level hazard is a system level causal factor. When analysing the interfaces both the following viewpoints must be taken and aligned; the sub-system "sees" a hazard on the (sub)- system boundary, while the systems integrator "sees" an interface hazard. They are one and the same thing but must be accounted for in both the "up" (integration) and "down" (devolution) directions.

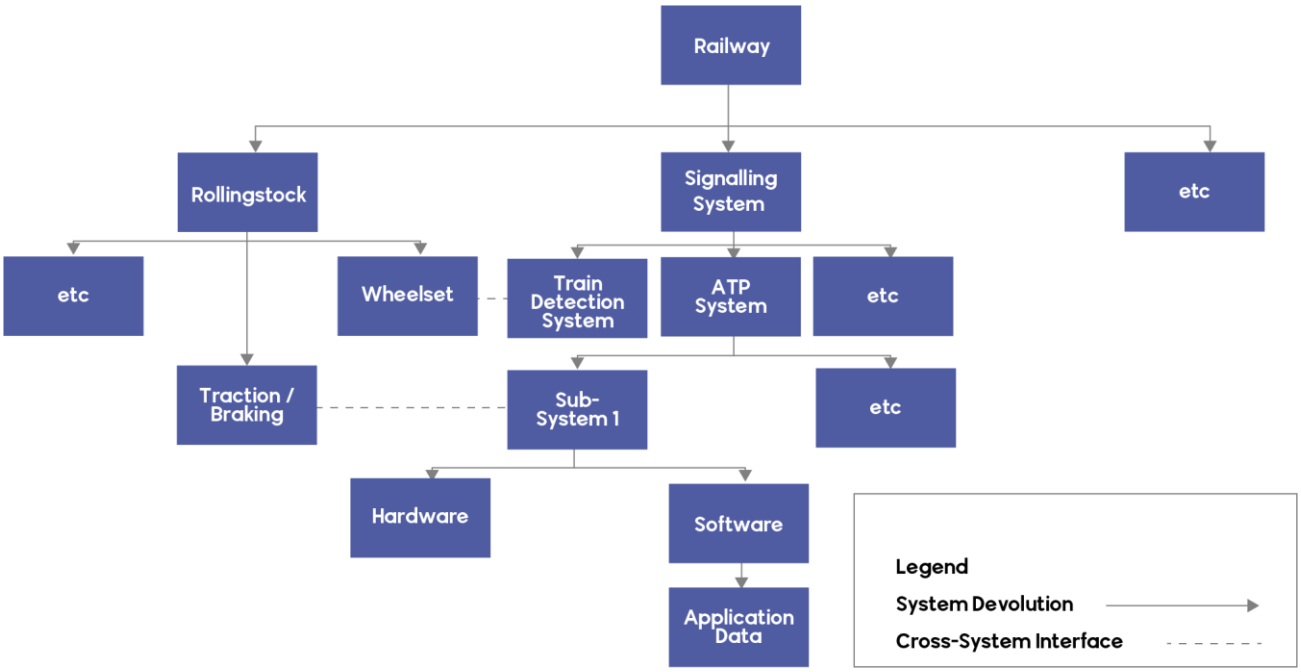

Figure 4 Devolution into a "System-of-Subsystems"

Another key point to note is that projects are usually delivered by various parties such as a customer who performs the overall definition and setting of objectives and high-level operational requirements etc. and one or more contractors and sub-contractors who are responsible for various lower level parts. From a systems engineering point of view, this partitioning of responsibilities and devolution of the delivered system is done by (or receives major input from) a systems architect role who always maintains a broad view over the entire system and project.

This is sometimes portrayed as a "system-of-systems" approach where the opportunity for such close and detailed oversight of these interfaces and apportionment of requirements etc. is often problematic. These issues can be mitigated by the adoption of the strategies recommended in section 4.7 above.

For engineering safety management to be fully effective, there must be a similar role to the systems architect (often also known as a system integrator). They are someone or some group that follows the lifecycle of the project and system safety activities at all levels even though the detailed work is done by others either within the customer or within the various contractors and suppliers, to ensure that there are no "gaps" in the engineering safety management work. This is a prime instance of all the iESM "Working with Suppliers" fundamentals.

5.2 Key System Integration Activities

Systems integration is not something that happens as if by magic, from the "bottom-up", towards the end of a project. Systems integration starts at the planning and requirements capture phases and extends through the architecture and detailed design phases, the implementation phase and the "conventional" integration phase. For a system to be integratable, it must firstly be specified and designed to be so. It must be initiated from the "top-down" so that the "bottom-up" stages work effectively.
It should be noted that Systems Integration takes time and effort at the start of the project and may appear to occupy resources with no apparent delivery of project artefacts. If Systems Integration is performed well, then the time taken with no apparent delivery at the start of the project will result in a project that works correctly and will require minimal remedial attention at the end of the project, thus saving both time, and physical and financial resources, as well as achieving good customer relations.

A comprehensive set of System Integration activities, which are required to support a complex programme of delivery project, is likely to include the following:

- **System Integration Strategy** – that sets out the System Integration objectives (e.g. to gain an increasing level of confidence (as integration progresses) that the delivered system will meets its requirements and end purpose) within the context of the project and sets out the way that the System Integration activities will meet their objectives and what proof of successful integration is required at each stage. This may be developed into a System Integration Management Plan or integrated into the Project Plan for smaller projects.
- **System analysis & requirements** – This analysis is conducted to determine how the emergent properties of top-level performance may be satisfied with procured rolling stock and infrastructure which will lead to a set of requirements that should interface directly with delivery project scope. Modelling is often an important part of systems analysis.
- **Modelling** – it is likely that a range of modelling may be required such as performance modelling (e.g. Vision), RAM modelling e.g. TRAIL, safety modelling (e.g. fault trees, consequence trees). Modelling is often used to help decompose requirements, test the performance of emerging design options, help understand critical issues, examine change requests and determine the impact of non-compliances. The degree to which modelling is validated and may be relied upon is an important factor.
- **Systems design & specification** – For major programmes there are often a number of stages of analysis and design before the requirements for individual projects can be specified. Typically, there may be a need for an overall railway specification which would encompass an overall architectural solution at the railway level, and this can then be broken down into geographical and/or functional projects.
- **System assurance** – Such assurance provides confidence that requirements will be satisfied. This is often split into safety and verification and validation streams of activities.
- **Engineering Safety Management** – analysis of the safety attributes of the project and or systems deployed. This usually starts with the identification of potential hazards and leads to production of a safety case showing how the design satisfies the overall safety objectives.
- **Programme V&V** – the Verification and Validation activities will provide evidence that top level requirements have been decomposed in the design moving down the left-hand side of a system lifecycle and validation activities will confirm that the emerging system/infrastructure satisfies the requirements. Sometimes programmes employ an additional independent V&V activity (IV&V).
- **System acceptance** – Assurance, including safety assurance is often paper intensive and technically challenging. Successful projects usually identify all stakeholders who have a role to play in acceptance of deliverables and plan and project manage the acceptance process.
- **Configuration & Data Management** – is essential to confirm that a set of requirements, design documentation and the resultant system all relate to a particular version of deliverables that are being delivered. The configuration and data management processes (and often supporting tools) need to manage the version of each deliverable and the relationship between different elements often referred to as configuration items.
- **Technology** – this is a generic heading to pick up the provision of new (or modified) developments or the new (or modified) application of existing developments. This aspect of any project is often high risk and needs management arrangements and competencies beyond those required by a conventional application design and implementation project.
- **Operations & Maintenance Engineering processes** – projects usually need to provide the wherewithal to manage infrastructure throughout its operational life. This stream of activities comprises the processes, tools, training, competency criteria etc. for routine operations and maintenance and the ability to handle abnormal and failure conditions. Often the latter may be done through second- or third-line support contracts.
- **Critical Issues Process** – the technical issues that lead to project risks may range from uncertainty to declared non-compliance with requirements or the inability to deliver top level objectives with the emerging design. A process is required to manage, prioritise and resolve critical issues. There should be a strong link between the critical issues process and programme risk assessment and management.

- **Design Assurance** – As routine design is emerging it needs to be assured by demonstrating compliance with project requirements and applicable standards. This will be the project level contribution to the overall V&V arrangements.
- **Interface Working groups** – interfaces are known risk areas and it is usual practice to establish interface working groups to cooperatively specify, agree and deliver to specifications of the interface covering form, fit and function.
- **Start of Service/Operational Readiness** – projects are often scoped in terms of physical deliverables and, to avoid the possibility that the soft/process arrangements are lacking or not integrated, recent practice is to establish a stream of activity to identify and manage everything necessary to start and run an operational service. This is best done through the eyes of the operator rather than the delivery team.
- **System Level Trade-offs** – although this activity could be assumed to be inherent in those above, it is drawn out to make it explicit. As major programmes are complex and often last over a long time period, it is usual to need analysis of:
    - Emerging non-compliances
    - Design and/or implementation options in relation to cost/risk issues
    - Changed stakeholder requirements
    - Formal Change Management – beyond the management of configuration there needs to be a formal process for accepting requests to change the scope of the project or the current approved design, assessing the consequences and agreeing to or rejecting changes. The Formal Change process often works through a senior level change board as it is necessary to integrate technical, project management and commercial matters. Even committing resource to considering a proposed change can have significant cost, resource and timescale implications.
- **Competency Management** – Work is done by people. They may be assisted by tools, processes and procedures, but it is only people who actually produce and justify the safe system. There needs to be a formalised and independently assessed competency management system applied to those people undertaking the key works of the project. There are existing competency definitions and models for safety-related system practitioners [6] and for systems engineers [7].
- **Ergonomics and Human Factors** – Humans are a part of almost every system. They provide inputs (controls) into a system, and reads and act upon system outputs (indications). They also perform diagnostics and maintenance on the system. Any error (input to, or reading and acting upon an indication) must be considered as a possible cause of a hazard as should any error in a maintenance activity. System maintainers could also be exposed to a hazardous emission (e.g. radiation, or toxic/noxious substances). System integration must extend to the humans who interact with the system in any way.

6 LIFECYCLE PHASES

It is important to note that while the following describes “a single pass” through the lifecycle activities, most projects have a multi-stage and blended life cycle where Project Definition takes place only once (even if this is iterative towards a final singular definition), but the particular definition may consist of several repetitions of the remaining phases as, for example, geographic coverage is expanded, and/or further functionality is delivered.

In order to illustrate the parallels between iESM [1] and EN50126 [2], we will use the following diagrams in Figures 6 and 7, highlighted at each lifecycle phase, to indicate the relationship between these two lifecycle models. The relationship between iESM [1], EN50126 [2] (and IEC 15288 [5]) is not hard and fast. There are overlaps and this is indicative of the differing viewpoints of each document. The lack of a definitive one-to-one or even one-to-many mapping between these documents should not be cause for concern. Throughout we will adopt a “risk-based” approach where the most effort is put in the areas with the highest potential risk.

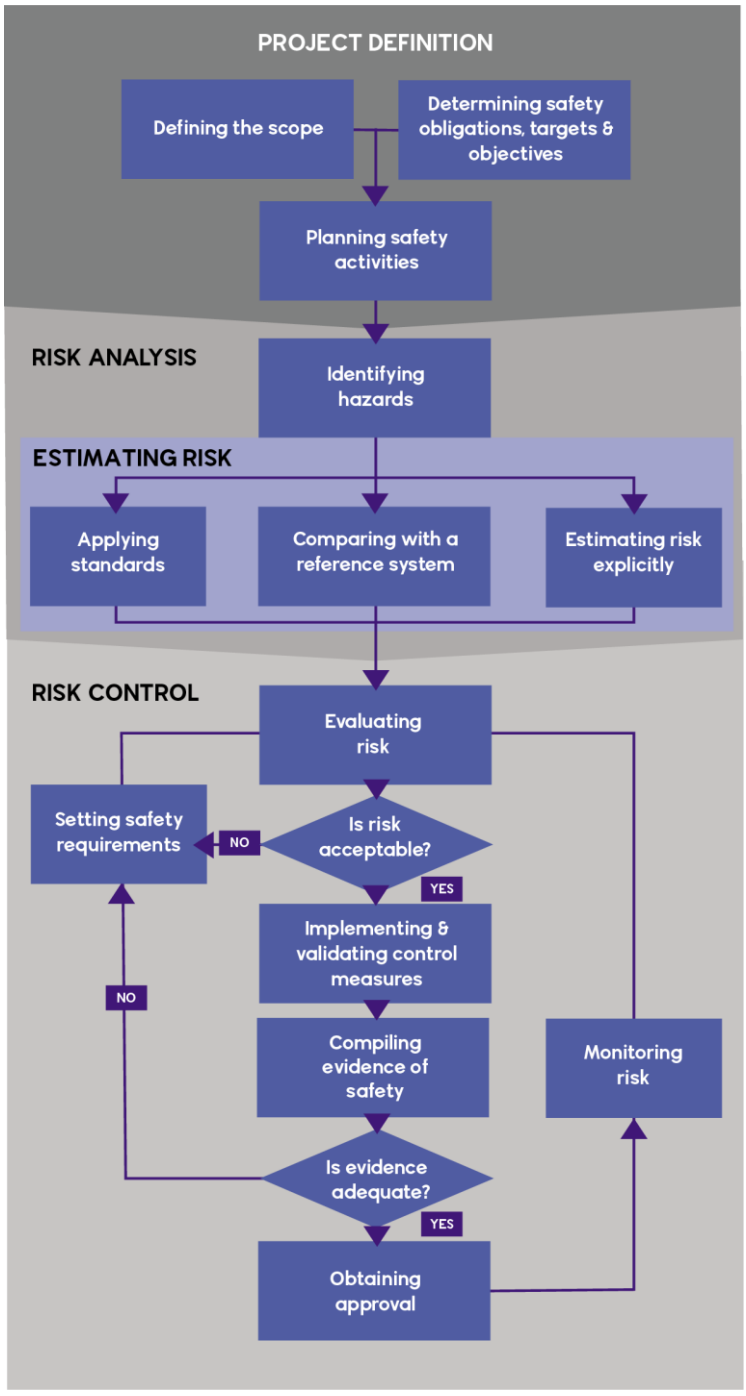

Figure 5 iESM Lifecycle Model

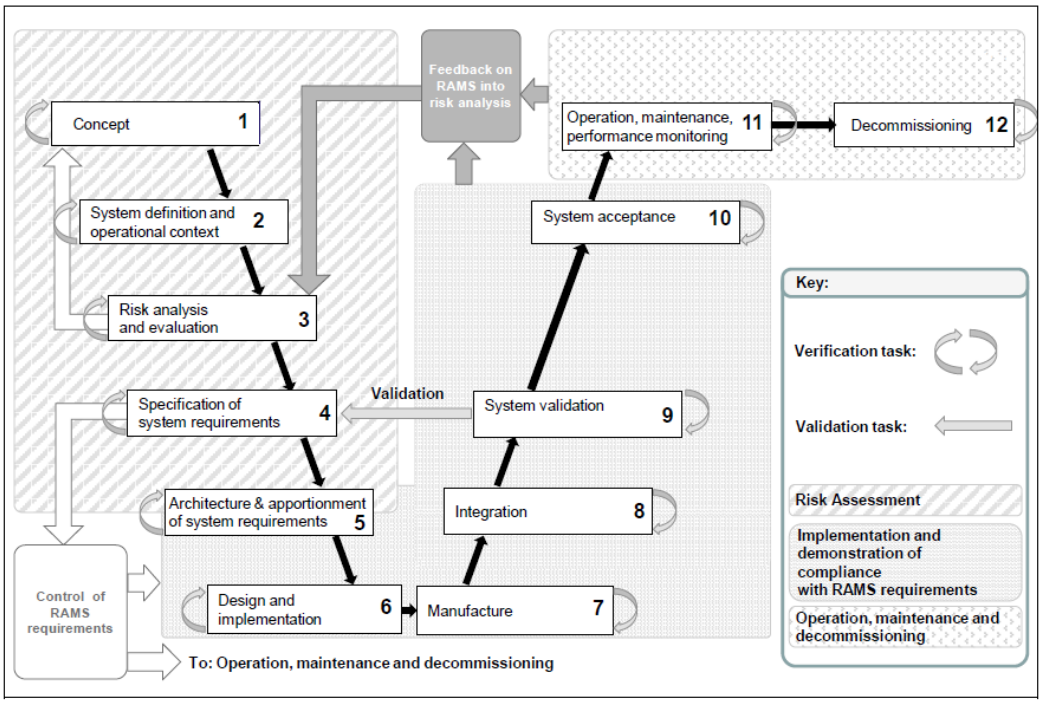

Figure 6 EN50126 Lifecycle Model

Readers who are familiar with the evolution of the EN50126 standard will recognize that while there have been some changes between the 2001 and 2017 versions of the standard, these changes are more by way of re-arrangement and consolidation, rather than fundamental changes, with the only significant change being the inclusion of the use of codes of practice and use of a similar reference system as allowable methods of risk estimation (in addition to the original, 2001 version, explicit risk estimation). This enhancement brought EN50126 into alignment with the Common Safety Method on Risk Evaluation and Assessment (Europe) and the fundamentals of iESM.

Note that in the following sections, we assume a documentation structure as per Figure 8 which is reflective of the independence requirements for SIL 3 & SIL 4 functions as shown in EN50128 [3] at Figure 2. Other structures may be valid; however the key is to know what the documentation structure is, what each document is to contain, and the relationship (parent, peer or input) between documents in the structure.

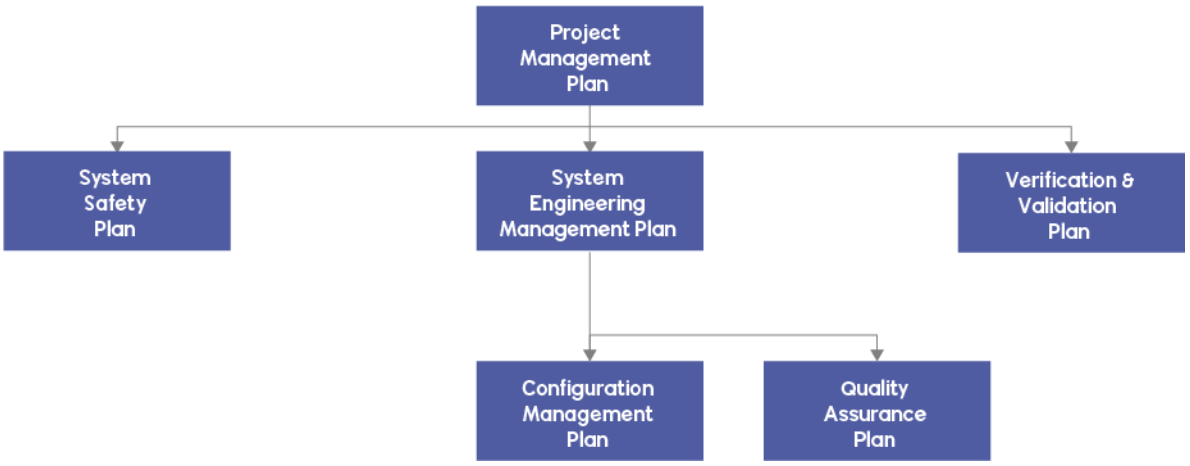

Figure 7 Indicative Documentation Structure

6.1 Project Definition

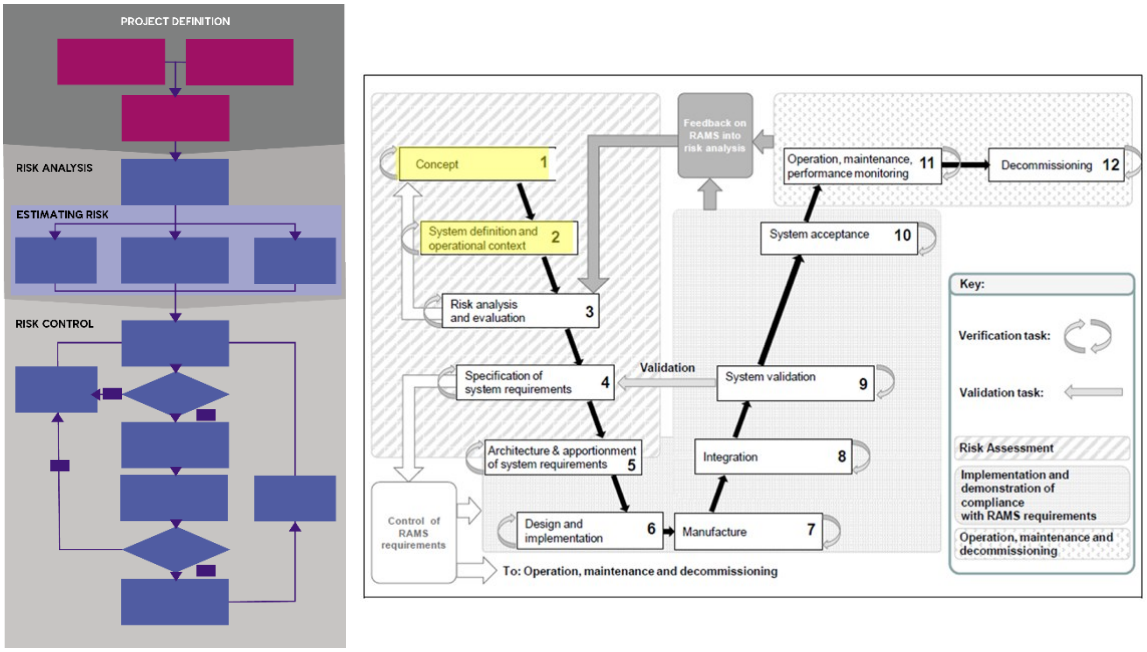

Figure 9 Project Definition Lifecycle Comparison (Project Definition)

During this phase (the equivalent of CENELEC phases 1 Concept and part of 2 System Definition): -

- Project management will:
    - Confirm the overall concept and project program which must include the specification of any intermediate milestones for progressive delivery of the project (such as an expanding geographic scope of application, incremental delivery of an increasing range of functionality, etc.). These will ultimately be documented and communicated in the top-level planning document often known as a Project Management Plan (or similar). See [5] clause 6.3.1 for further guidance.
    - Set in place those cross-lifecycle activities such as Competency Management, Quality Management (in accordance with either ISO9001 [8] or ISO10006 [9] as best fits the project) and Configuration Management (in accordance with ISO10007 [10]). See iESM [1] sections 19, 20, and 21 for further guidance.
    - Specify and document the required inter-relationships between the various groups/roles involved in the project's delivery. This is often documented as a RACI (Responsibility, Accountability, Consultation and Input) matrix which may be part of the Project Management Plan or a separate document to be managed and maintained through the life of the project. See iESM [1] section 19 for further guidance on safety roles and responsibilities.

- Systems engineering will:
    - Develop, from the Project Management Plan, a second-level planning document often known as a System Engineering Management Plan or Design Management Plan (or similar).
    - Describe the way in which the delivered system will operate (and be operated and maintained). These will be recorded in such documents as a Concept of Operation.
    - Specify a system architecture which identifies the various sub-systems/products and the way they are interfaced together in order to achieve the project's objectives. In most projects this will involve the selection of existing products/sub-systems to be used "as-is", modified in particular ways in order to meet the project objectives, or developed from new.
    - Establish the requirements management and traceability processes.

- Provide input to project management into the development of the project program.
- Provide input to project management into the development of the Configuration Management Plan.

- Engineering safety management will:
  - Start from the implicit assumption that all other actors in the project are aware of the activities and benefits of engineering safety management, however, if this assumption is not valid on the particular project, then provide a presentation/briefing to project management and systems engineering on the generic activities of engineering safety management indicating the role it plays within the overall success of the project and the necessary communication and interaction required with all parties in order for engineering safety management to be effective. This will assist in promoting a safety culture within the entire project.
  - Provide input into the development of other management plans such as the Project Management Plan, System Engineering Management Plan (or similar), Verification and Validation Plan, Quality Assurance Plan, Configuration Management Plan etc. and be a part of the internal review and approval audience of such documents. See iESM [1] sections 11 and 18 for further guidance.
  - Obtain or otherwise determine the safety obligations, targets and objectives. See iESM [1] at section 8.2.9 and EN50126 [2] at Annex C for further discussion on risk acceptance. Note also that your local regulatory environment may place additional obligations on the project, particularly in relation to a requirement to assure that risk is reduced As Low As Reasonably Practicable or So Far As Is Reasonably Practicable – two very similar concepts. Any local regulatory advice on this issue should be followed.
  - Develop a System Safety Plan (which is consistent with the Project Management Plan, System Engineering Management Plan (or similar), Verification and Validation Plan, Quality Assurance Plan, Configuration Management Plan etc.). See iESM [1] section 6 for further guidance.
  - Establish their role as a member of the project Change Control Board for Configuration Management purposes (see IS0 10007 [10]). Consideration may also be given on complex and/or high-risk projects, to having the Independent Professional Reviewer sit on the CCB as an observer. See iESM [1] section 18 for further guidance.
  - Select a suitably independent, competent and experienced Independent Professional Reviewer and with them, develop a scope of work and remit which provides necessary coverage of all areas where engineering safety risk on the project may arise, and a reporting regime and schedule which aligns with the overall project program. developed by project management. See iESM [1] section 17 and iESM Application Note 4 for further guidance.
  - Work with the Regulator (if your legislative regime has one) to define a mutually agreeable method of acceptance and approval of the delivered system.
  - If consistent with a local co-regulatory regime, then as an alternative, it is good practice at this point to contact the relevant regulatory authorities and brief them on the project and the project strategy for achieving and demonstrating the safety of the delivered system within the railway systems environment including the development of a program of regulatory engagement activities. See iESM [1] section 14 for further guidance.

- Independent Professional Review will:
  - (Ideally) assist in the detailed development of the scope and remit of their activities defining the objectives to be achieved (the WHAT and the WHY), based upon the project briefing provided by engineering safety management and systems engineering. See iESM Application Note 4 for further guidance.
  - Develop an Assessment Plan defining the HOW, the WHO and the WHEN of the Independent Professional Reviewer's activities for the project's approval. See iESM Application Note 4 for further guidance.

As part of the verification activities, it is good practice for project management to conduct a “gate review” at the end of each project phase which, among other objectives, should have the objectives of ensuring that all activities planned for this phase have been completed (and formally approved where necessary), and that the results from the many workstreams are consistent with each other and also with the originally-stated project objectives. It is good practice to have an alignment between project phases and these CENELEC lifecycle phases. This alignment need not be one-to-one, but each project phase should align with the completion of a CENELEC lifecycle phase. Activities in the next phase (either project phase or CENELEC lifecycle phase) should not be allowed to begin (or at worst, be allowed to proceed only to a limited extent and under close monitoring) unless and until this gate review is satisfactorily achieved.

6.2 Systems Specification & Requirements

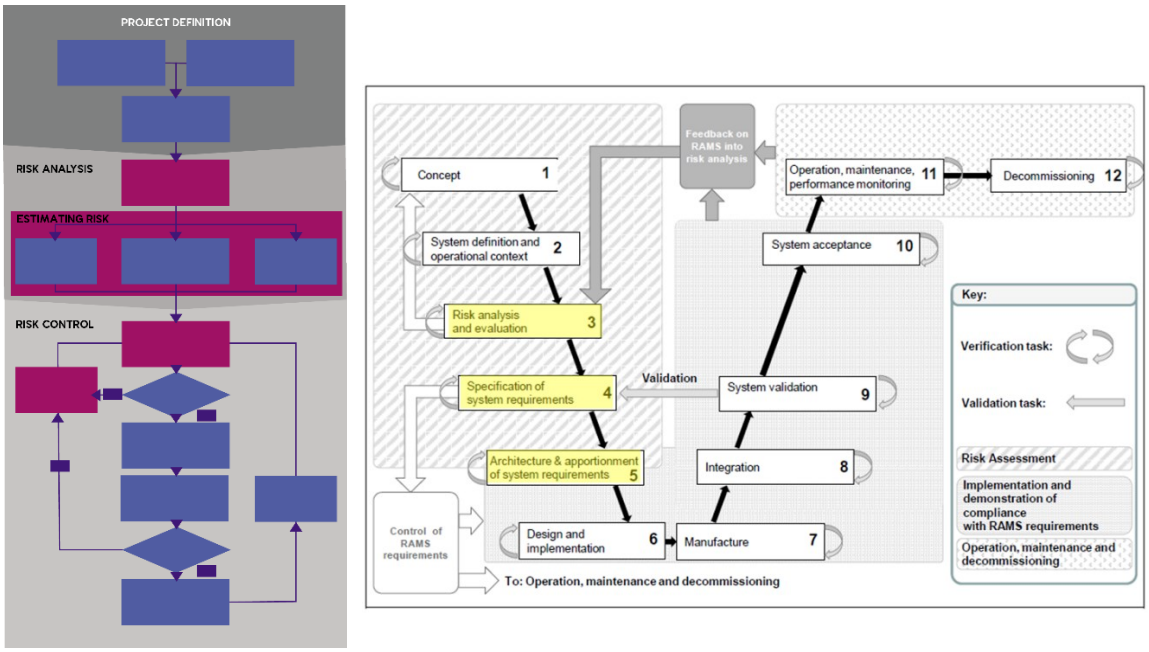

Figure 10 - Project Specification Lifecycle Comparison (System Specifications & Requirements)

During this phase (the equivalent of CENELEC phases 3 Risk Analysis, 4 Specification of System Requirements, and 5 Architecture and Apportionment of System Requirements):

- Project management will:
  - Implement their Project Management Plan monitoring the progress of the various workstreams and managing any external contractors engaged at this point.
  - Implement their Configuration Management Plan.

- Systems engineering will:
  - Develop a System Requirements Specification and from this, they will be decomposing the delivered system into its various elements (sub-systems) as per the “system-of-systems” approach indicated above. This decomposition process produces a System Architecture and Design document, which leads on to the various Sub-system/Element Requirements Specifications and an Interface Requirements Specification for each interface. See [5] clause 6.4.3 for further guidance.
  - Prepare a Verification and Validation Plan See [5] clauses 6.4.9 and 6.4.11 for further guidance.

- Establish and operate the Data Reporting, Analysis, and Corrective Action System (DRACAS) process (as part of the ISO55001 [11] management of the asset). Failure Reporting, Analysis, and Corrective Action System (FRACAS) may be considered to be a subset of DRACAS (looking only at failures rather than any and all relevant system/operational data). MIL-HDBK-2155 [12] provides some insight into the requirements and operation of a FRACAS. The iESM Application Note 3 "Tools and Techniques" [13] also contains information on DRACAS.

- Engineering Safety Management will:
  - Establish the safety risk acceptability criteria for the delivered system. See iESM [1] section 5 for further guidance.
  - Identify the top-level hazards, and their various causes at a high level (with input from an appropriate group of subject matter experts covering all relevant competencies and disciplines which may include such specialisms as human-factors, signalling, EMC, practitioner), See iESM [1] section 7 for further guidance.
  - Identify the interface / sub-system level hazards which should be traceable to the causes of top-level hazards (see figure 4 above).
  - Identify safety requirements to control each cause of an identified hazard (a causal control), See iESM [1] section 9 for further guidance.
  - Identify safety requirements to limit the extent to which a hazard may result in an accident (a consequence control or barrier to escalation).
  - Apportion top level safety targets to top hazardous events (if these have not been provided by the railway owner). This assumes that the railway organisation has a hazard log and basic fault tree which models their overall risk. This apportionment is a slice of this overall risk allocated to the works of the project. See iESM [1] section 8 and clause 9.2.3 for further guidance.
  - Allocate Safety Integrity Levels (SILs) to safety functions. (See iESM [1] at section 9.2.4 and 9.2.6 for further guidance and IEC61508-5 [14] for methods of SIL allocation.)
  - Establish the delivered system's Hazard Log. See iESM [1] clause 16.2 and iESM Application Note 9 for further guidance.
  - Ensure that these safety requirements are captured in the system engineering requirements management processes.
  - Establish a process for the capture, verification and monitoring of Assumptions and Caveats relied upon for the safety of the delivered system. See iESM [1] clause 16.2.3 and 16.2.4 for further guidance.
  - Establish a process for the capture of either residual risks or Safety Related Application Conditions (Dependencies) and their transfer to, and acceptance by suitable others (potentially the owner, operator and/or maintainer of the delivered system). This transfer process is a two-way activity with the required end result that those who are in the best position to accept and manage the residual risk (or to implement the SRAC that applies to the residual risk) are aware of what they need to do in order to adequately manage risk in the long term.
  - Where the scope of the project requires or implies it, confirm that the fulfilment/implementation of these Safety Related Application Conditions is subject to Verification and Validation by systems engineering.
  - Maintain oversight of the scoping, specification, and conduct of any engineering safety management activities performed by contractors or suppliers.
  - Take part in the review audience for the various Requirements Specifications and the Verification and Validation Plan.
  - Potentially commence the preparation of a Cross-Acceptance argument (evidence of safety based on an existing certificate or approval). See iESM [1] section 12 for further guidance.
  - Potentially update the System Safety Plan.
  - Potentially facilitate the assessment and auditing works of the Independent Professional Reviewer.
  - Potentially address issues raised by the Independent Professional Reviewer noting that some of these items may relate to activities and work products provided by systems engineering or project management.

- Potentially producing a concept safety case arguing that all hazards have been identified and all safety requirements established.

- Independent Professional Review will:
  - implement their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of tests, and the production of the required reports.

6.3 Design

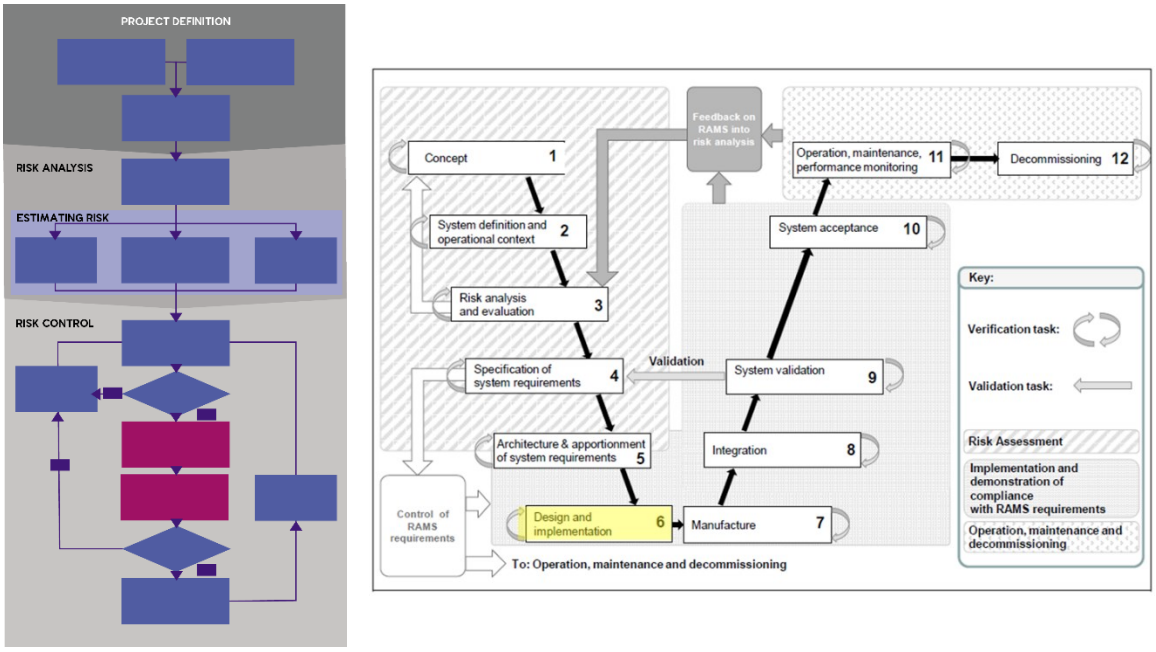

Figure 11 - Project Definition Lifecycle Comparison (Design)

During this phase (the equivalent of CENELEC phase 6 Design): -

- Project management will:
  - Implement their Project Management Plan monitoring the progress of the various workstreams and managing any external contractors engaged at this point.

- Systems engineering will:
  - Develop the necessary element and Interface Requirements Specifications and Design Specifications. See [5] clauses 6.4.4 and 6.4.5 for further guidance.

- Engineering safety management will:
  - Maintain oversight of the scoping, specification, and conduct of any engineering safety management activities performed by contractors or suppliers.
  - Be part of the review audience for the various Design and Interface Specifications.
  - Conduct Interface Hazard Analysis on the internal and external system interfaces.
  - Conduct an O&SHA (Operation & Support Hazard Analysis) on the human interactions with the delivered system, if any. See iESM Application Note 1 for further guidance in relation to O&SHA checklists.

- Confirm whether adequate fault management measures are being provided, such as built-in-test and diagnostic facilities, as well as maintenance functions.
- Confirm that system engineering will provide adequate maintainer, and operator training as well as adequate operations and maintenance procedures which satisfy all relevant SRACs.
- Monitor the design process to identify any arising hazard causes (potentially as a result of design decisions) and to action any new required control measures.
- Update the Hazard Log.
- Potentially update the System Safety Plan.
- Facilitate the assessment and auditing works of the project by the Independent Professional Reviewer.
- Address issues raised by the Independent Professional Reviewer noting that some of these items may relate to activities and work products provided by systems engineering or project management or that will be addressed in the future.
- Potentially produce an emerging safety case arguing that all safety requirements have been incorporated into the design.

- Independent Professional Review will:
  - Implement their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of tests and the production of the required reports.

6.4 Implementation/Integration

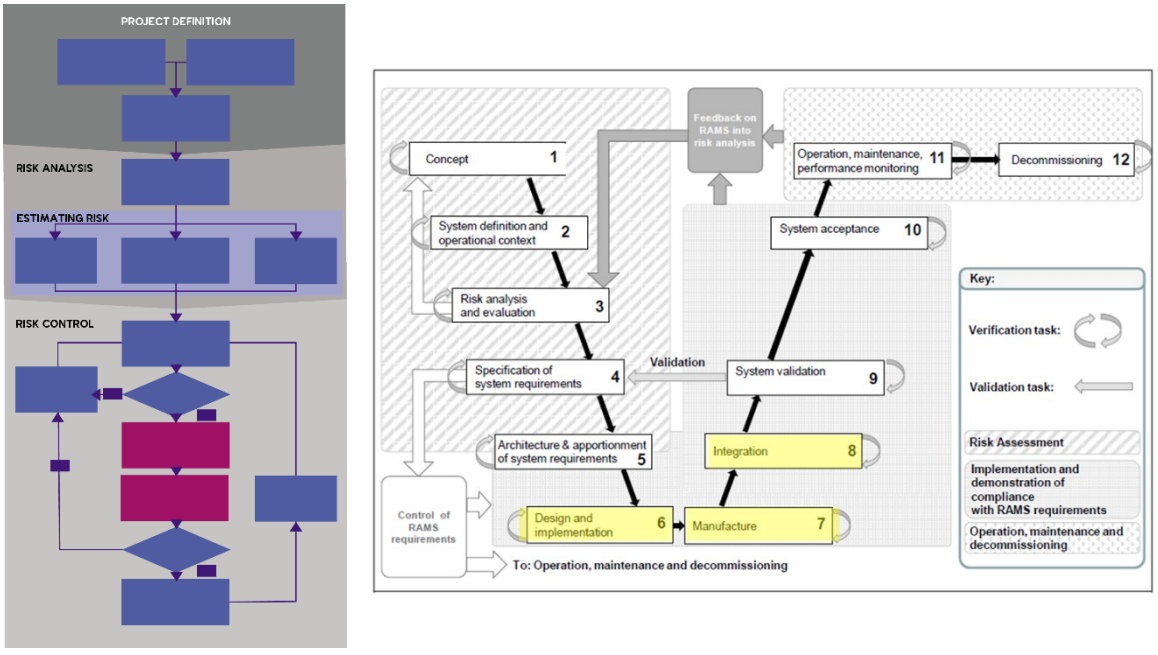

Figure 12 – Project Definition Lifecycle Comparison (Implementation/Integration)

During this phase (the equivalent of CENELEC phases 6 Implementation, 7 Manufacture, and 8 Integration):

- Project management will be implementing their Project Management Plan monitoring the progress of the various workstreams and managing any external contractors engaged at this point.

- Systems engineering will:
    - Oversee the implementation from manufacture to installation of all the delivered system elements and requirements as designed. See [5] clause 6.4.7 for further guidance.
    - Produce systems integration plans. See [5] clause 6.4.8 for further guidance.
    - Manage the traceability of all requirements to inspection and test records.
    - Produce requirements traceability reports indicating that all requirements are implemented, that the design is uniquely traceable to the requirements and that all non-trivial assumptions are traced to SRACs.
    - Conduct system integration.
    - Demonstrate that the delivered system has been integrated into any pre-existing system within the railway operational context with no undesired effects.
    - Produce system integration reports.

- Engineering safety management will:
    - Maintain oversight of the scoping, specification, and conduct of any engineering safety management activities performed by contractors or suppliers.
    - Be part of the document reviewing team for the integration plans and integration reports.
    - Liaise with the Verification and Validation role within the project to track the progress of validation of safety requirements.
    - Update the hazard log with the evidence of validation of safety requirements.
    - Potentially participate in any audits of the project activities (from a safety point of view).
    - Potentially witness integration testing (representing the safety viewpoint) and produce or contribute towards the production by others of, the Integration Report(s).
    - Potentially update the System Safety Plan.
    - Facilitate the assessment and auditing of the project by the Independent Professional Reviewer.
    - Address issues raised by the Independent Professional Reviewer noting that some of these items may relate to activities and work products provided by systems engineering or project management.
    - Potentially produce an update to the emerging safety case arguing that all implementation has not jeopardised the integrity of the design.
    - Confirm the correctness of the traceability reports.

- Independent Professional Review will:
    - Implement their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of tests and the production of the required reports.

6.5 System Validation & Acceptance

It should be noted that System Integration and System Validation are often interlinked and run concurrently over an extended period of time which may commence at Factory testing and extend into Site testing and through to commissioning. Before site activities (construction, installation, testing and trialing) are carried out, there should be an identification of risks, both to the persons carrying out the activities and to any existing railway operations. These risk assessments must take into account how much reliance is being placed on the system for safety at each stage of such testing. Such risks shall be managed to an acceptable level. Documentation shall be produced and submitted as required to demonstrate appropriate management of risk. As soon as testing extends beyond laboratory or factory testing to site testing, it is good practice to develop a safety assurance statement (which may be as detailed as a Safety Case) in order to assure that the risks associated with such testing events are acceptable. Risks associated with occupational health and safety (OH&S) or workplace health and safety (WHS) shall be communicated to the relevant parties.

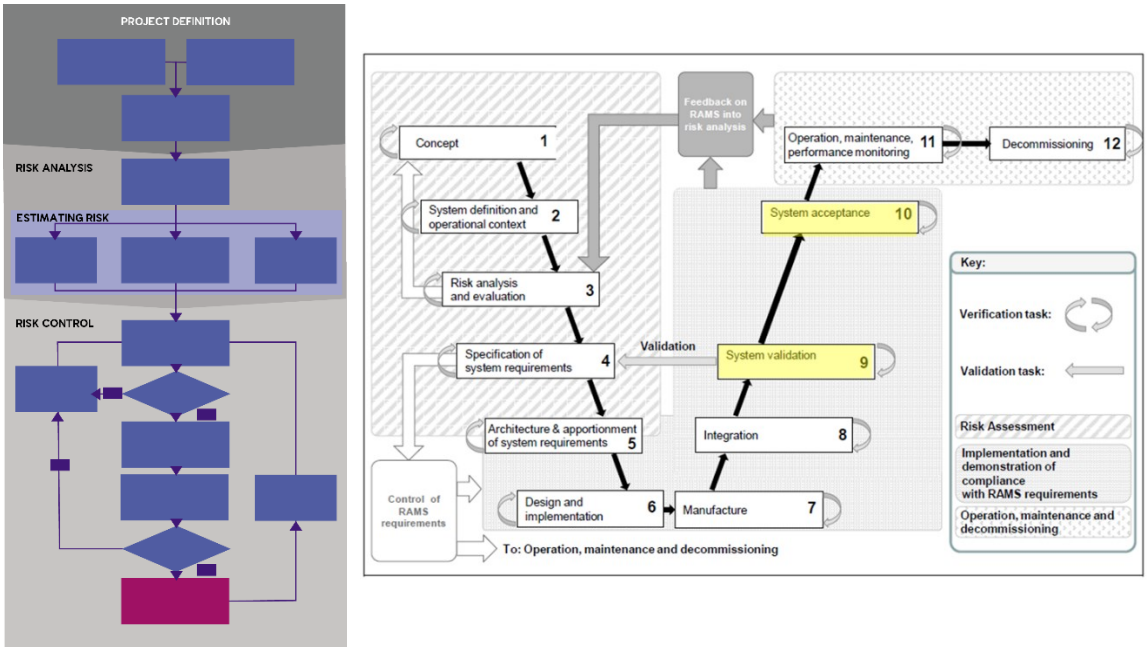

Figure 13 - Project Definition Lifecycle Comparison (Validation & Acceptance)

During this phase (the equivalent of CENELEC phases 9 System Validation, and 10 System Acceptance):

- Project management will be implementing their Project Management Plan monitoring the progress of the various workstreams and managing any external contractors engaged at this point.

- Systems engineering will:
  - Conduct the planned validation activities See [5] clause 6.4.11 for further guidance.
  - Maintain an up-to-date log linking each requirement against its validation evidence.
  - For signalling systems this will include tests against documented signalling principles.
  - Operate the DRACAS.
  - Implement corrective action for requirements that have not been successfully validated.
  - Plan and implement regression testing while corrective actions are being applied to the delivered system.
  - Produce the required verification reports.
  - Produce the required validation reports.

- Engineering safety management will:
  - Maintain oversight of the scoping, specification, and conduct of any engineering safety management activities performed by contractors or suppliers.
  - Conduct an identification of hazards, arising from the delivered system, to persons carrying out the testing and trialing activities. Risks arising shall be discussed with system engineering and appropriate control measures identified and implemented.
  - Confirm whether adequate operator training and adequate operational and maintenance procedures are provided which satisfy all the related SRAC's (and advise the Verification and Validation Role if they are not).
  - Liaise with the Verification and Validation role within the project to track the progress of validation of safety requirements.
  - Monitor safety (via the DRACAS) such as the existence and rate of wrong side failures or design errors emerging during testing.
  - Update the hazard log with the evidence of compliance with safety requirements.
  - Be part of the review audience for the verification reports and validation reports.
  - Potentially participate in any audits of the project activities (from a safety point of view).

- Potentially witness validation activities (representing the safety viewpoint) and produce or contribute towards the production by others of, the Validation Reports.
- Potentially update the System Safety Plan.
- Facilitate the assessment and auditing of the project by the Independent Professional Reviewer.
- Address issues raised by the Independent Professional Reviewer noting that some of these items may relate to activities and work products provided by systems engineering or project management.
- Develop any safety assurance statements required to cover testing/validation activities.
- Develop the Safety Case for the particular release of the delivered system being accepted (for all functions) into service arguing that the delivered system meets it safety targets and obligations (or will do so once the planned commissioning activities have all been successfully completed) and that all SRAC's have been transferred to, and discharged by, those who are appropriately responsible for doing so. See iESM [1] sections 12, 13, and 14 for further guidance.

- Independent Professional Review will be implementing their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of tests and the production of the required reports.

6.6 Operation & Maintenance

Not all projects extend into the operation and maintenance phase. Some projects undertaken via a contract often have a defects liability (or warranty) period which extends past the final commissioning and into this phase, but at some point, the contract ends and responsibility for the delivered system or asset transfers to the asset owner, operator and maintainer.

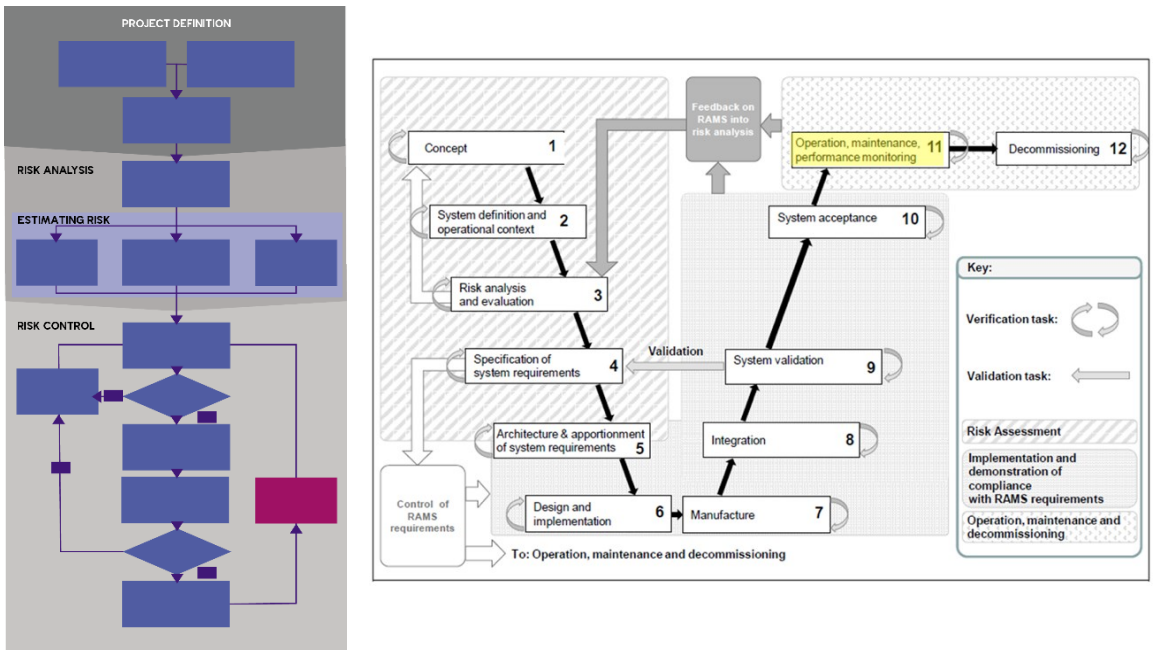

Figure 14 – Project Definition Lifecycle Comparison (Operation & Maintenance)

During this phase (the equivalent of CENELEC phase 11 Operation, maintenance and performance monitoring):

- Project management will not, as a specific function, be represented in this stage. The overall management of the delivered system will generally be shared between the asset owner, asset maintainer, and the delivered system's operator in accordance with IS055001 [11].

- Systems engineering will be operating the Data Reporting, Analysis, and Corrective Action System (DRACAS).

- Engineering safety management will be supporting the DRACAS process (as part of the ISO55001 [11] management of the asset) with a particular view to: –
    - Confirming that the delivered system is not failing more often than was originally specified or predicted. See iESM [1] section 15 for further guidance.
    - Confirming that the delivered system is not failing in ways that the analysis did not predict.
    - Confirming that the Safety Related Application Conditions relating to the ongoing monitoring of assumptions remain valid.
    - Confirming that the Assumptions and Caveats related to the delivered system's proof of safety are still valid.
    - Maintain oversight of the scoping, specification, and conduct of any engineering safety management activities performed by contractors or suppliers.

- Independent Professional Review will, if their remit extends to operational readiness, be implementing their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of tests and the production of the required reports.

6.7 Decommissioning and Disposal

Decommissioning and disposal are rarely done in isolation from the renewal and replacement of the decommissioned system. As such, this lifecycle phase is most often wrapped up into the initial lifecycle phase from Concept to Specification of Requirements. (EN50126 [2] or Definition to the early stages of Risk Control iESM) [1]).

It should be noted when a physical system is being decommissioned that, unless it is being turned off or removed in its entirety at a single stroke (which would be unusual for most railways), there will be intermediate stages of geographical extent and/or functionality that may not align with the original staging and hence, the delivered system, during decommissioning, may have a different set of hazards than it had during its installation and commissioning. It is even possible that some intermediate reduced scope configurations may be inoperable, unstable or extremely hazardous, so we have included the monitoring risk activity here in order to encourage projects to recognise this possibility and to monitor risks associated with those parts of the delivered system to be decommissioned (and even the interfaced systems which are not subject to decommissioning), to assure that risks at intermediate stages of decommissioning are understood and monitored.

For completeness, it is acknowledged that Disposal of some items of equipment may have environmental and/or occupational health & safety requirements which are outside of engineering safety management but nonetheless essential to ensuring safety. We will not comment further on these environmental or occupational health and safety matters other than to say that they must be considered, planned for, and dealt with in accordance with existing local regulations.

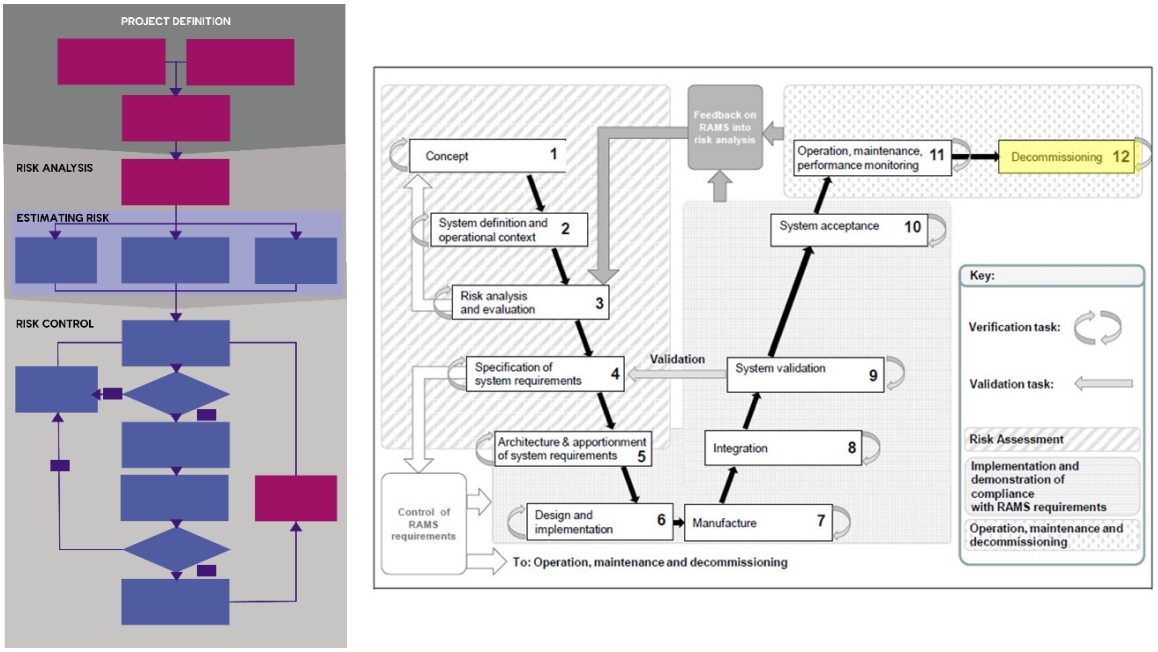

Figure 15 – Project Definition Lifecycle Comparison (Decommissioning & Disposal)

During this phase (the equivalent of CENELEC phase 12 Decommissioning): –

- Project management will be confirming the overall decommissioning strategy and project program which must include the specification of any intermediate milestones for progressive implementation of the project (such as a reducing geographic scope of application, and decreasing range of functionality, etc.). These will ultimately be documented and communicated in the top-level planning document often known as a Project Management Plan (or similar). They will also be setting in place those cross-lifecycle activities such as Competency Management, and Quality Management (in accordance with either ISO9001 [8] or ISO10006 [9] as best fits the project).

- Systems engineering will: –
    - Develop, from the Project Management Plan, their own second-level planning document often known as a Decommissioning Management Plan.
    - Describe the way in which the delivered system will operate (and be operated and maintained), under the progressive removal of functionality and/or geographical scope in order to achieve the project's objectives.

- Engineering safety management will:
    - Provide input into the planning of staging the decommissioning by conducting a hazard analysis on each proposed stage of the partially decommissioned system with a view to selecting the optimal decommissioning strategy/staging/sequencing.
    - Monitor the safety performance of the delivered system during its decommissioning and that of any interfacing systems which are not to be decommissioned.

- Independent Professional Review is normally not required for this phase in the railway industry, unless decommissioning and disposal is a part of a project to replace the existing system with a new one and the Independent Professional Reviewer has a remit which explicitly includes this Decommissioning and Disposal phase. Then the Independent Professional Reviewer will be implementing their Assessment Plan, which generally entails a series of document assessments, audits, witnessing of on-site activities, and the production of the required reports.

7 SUMMARY

This AN provides guidance on the working inter-relationship between engineering safety management, systems engineering and project management disciplines from the point of view of the ESM practitioner. It should be read in conjunction with iESM Guidance Volume 2 [1] which provides extensive information, background and guidance on the various methods, tools and techniques.

It has been written from a project life-cycle viewpoint, with reference comparisons made with EN50126 [2], by setting the engineering safety management activities in context with those of project management, systems engineering and independent professional review. In this respect, it may be read as an extension and expansion of Table 1 in EN50126 [2]. While there is no single "right way" to conduct engineering safety management activities on a project, experience has shown that there are many sub-optimal ways of doing so and this AN sets out to provide good practice so as to improve the chances of engineering safety success.

Railway history has shown the multiplicity of errors, omissions and inconsistencies which can lead to an embarrassing array of unfortunate outcomes. Reiterating these here is not necessarily helpful, nor is it aligned with the intent of this AN. Suffice it to say that, good outcomes are achieved by experienced, competent people, working together, rigorously following a robust and integrated suite of processes, supported by a set of validated tools, and overseen by knowledgeable project management, to achieve a desired outcome which is acceptably safe, and demonstrably so.

Implementing the guidance contained in this AN will, it is hoped, result in more effective, more integrated project activities and better system integration which should significantly reduce the likelihood of system safety "slipping between the gaps" of a poorly integrated system or a poorly integrated set of project activities.

8 REFERENCED DOCUMENTS

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

[1]	international Engineering Safety Management Volume 2 Methods, tools and techniques for projects
[2] [50126]	EN 50126:2017, Railway Applications – The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS), Part 1. Also issued as IEC62278.
[3] [50128]	EN 50128:2011 Railway Applications - Software for Railway Control and Protection Systems. Also Issued as IEC62279.
[4] [50129]	EN 50129: 2018, Railway Applications – Communication, Signalling and Processing Systems — Safety Related Electronic Systems for Signalling
[5] [IEC15288]	IEC15288:2015 “Systems and software engineering – System life cycle processes”
[6]	Competency Criteria for Safety-Related System Practitioners (IET)
[7]	”Systems Engineering Competencies Framework” INCOSE November 2016
[8] [ISO9001]	ISO9001:2015 “Quality management systems requirements”
[9] [ISO10006]	ISO10006:2017 “Quality management – Guidelines for quality management in projects”
[10] [ISO10007]	ISO 10007:2017 “Quality Management – Guidelines for configuration management”
[11] ISO55001]	ISO55001:2014 “Asset management – Requirements”
[12] MIL-HDBK-2155	“Failure Reporting and Corrective Action Taken” 1995
[13]	international Engineering Safety Management Application Note 3 “Tools and Techniques”
[14] IEC61508-5	“Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels” 2010

Note: This revision (Issue 1.1) of the Application Note has not modified any of the technical content present in the previous revision. Some of the standards referenced may have been revised. A full technical review is planned to be undertaken of this Application Note prior to its next revision.

iESM

BROUGHT TO YOU BY ARC

international Engineering Safety Management

Published on behalf of the international railway industry
by Abbott Risk Consulting Ltd.
Issue 1.1 May 2022

arc