Training in RAM Engineering

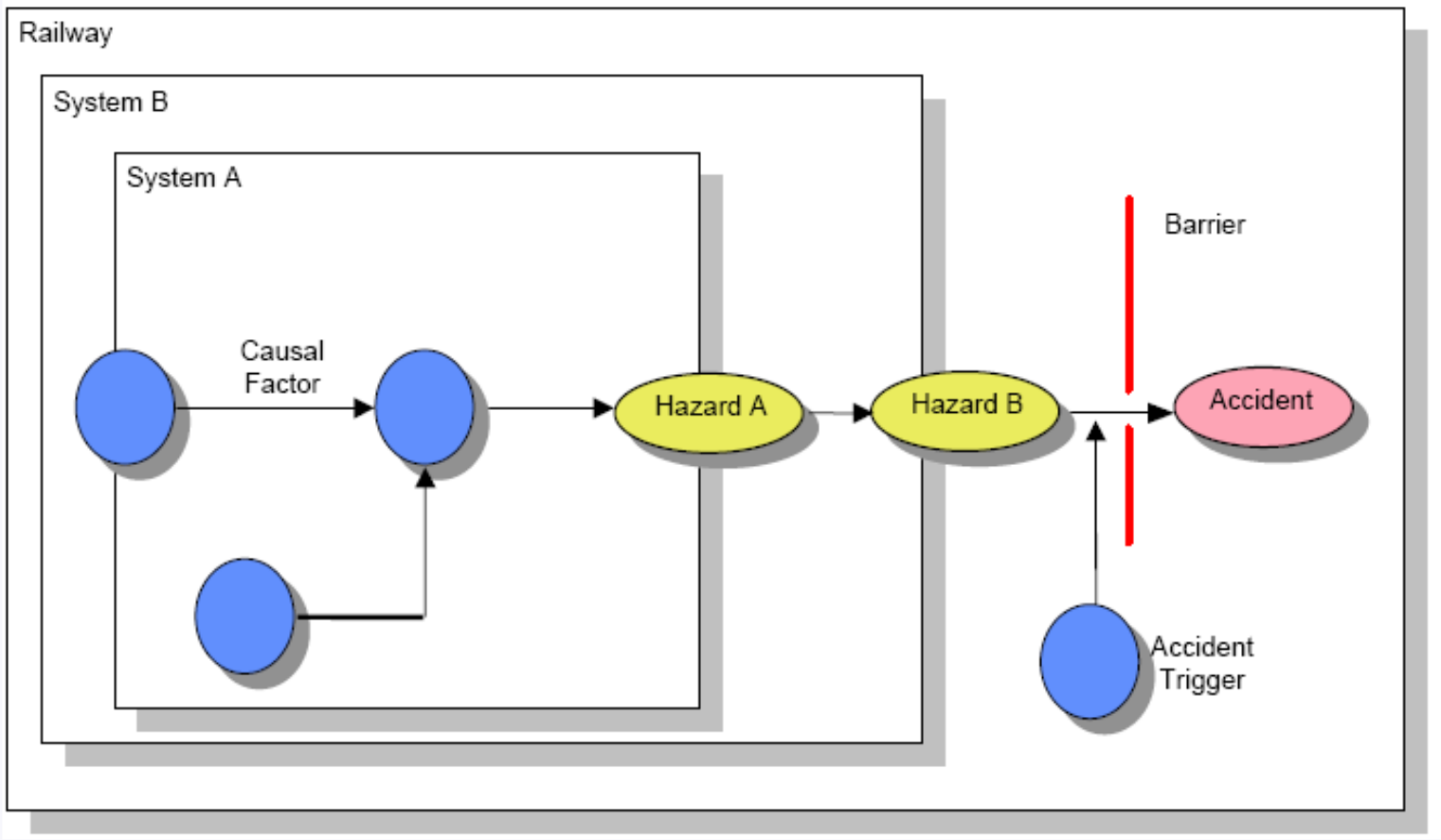
Delivering confidence in quality

Intellex RAMS Assurance consulting Ltd

Safety Engineering

- Engineering safety is not just done to meet the regulations
- Engineering safety ensures safety to its users and staff.
- Safer system brings reputation and productivity
- Safety is ensured through design, process and validation

Hazards


Railway
System B
System A
Causal
Factor
Hazard A
Hazard B
Barrier
Accident
Accident
Trigger

Definitions

Hazard definition

- Any situation that could contribute to an accident. Hazards should be eliminated wherever ‘practicable’, but this is not always the case. Where a hazard cannot be completely eliminated then there will be some risk.

Risk definition

- The likelihood that an accident will happen and the harm that could arise. In many cases, risk cannot be eliminated entirely. We must accept this if we are to continually improve safety..

Hazard Identification

HAZID

- Uses Hazard identification checklists. (e.g. in Appendix C section C.1)
- They may be applied to the whole system or to a component of it.
- Each item should be interpreted as widely as circumstances permit in the endeavour to unearth possible hazards.
- No checklist can be exhaustive and the analyst should bring his or her full experience to bear in searching for hazards.

Hazard Identification

HAZOP (Hazard and Operability Studies)

Where detailed design information is available and a high-level of assurance is required a Hazard and Operability Study or HAZOP can be carried out.

HAZOP is a systematic, creative examination of a design by a multi-disciplinary team.

The analyst should construct a Functional Block Diagram. At each level of indenture, this shows the components of the system or a sub-system, as blocks, with lines drawn between each pair of boxes that directly interact.

The team collects the design documentation, including a full functional breakdown of the system. Each component, including the interfaces, of the system is inspected in turn.

Hazard Analysis

Qualitative risk assessment

Qualitative risk assessment relies mainly upon domain expert judgement and past experience. Its advantages are

- it does not require detailed quantification, data collection or analytical work;
- it is relatively simple; and
- it is less expensive than quantitative risk assessment.

Its disadvantages are

- the assumptions require thorough documentation; and
- it is inadequate as the sole basis for assessment of major risks, including
- those arising from low loss incidents of high frequency, as well as from low
- frequency incidents associated with high losses.

Qualitative Assessment - Likelihood

- Frequent
- Probable
- Occasional
- Remote
- Improbable
- Incredible

A quantitative band may be defined for each category to facilitate estimation of the system risk

Qualitative Assessment -Severity

Catastrophic

Fatalities and/or multiple severe injuries and/or major damage to the environment

Critical

Single fatality and/or severe injury and/or significant damage to the environment

Marginal

Minor injury and/or significant threat to the environment

Insignificant

Possible minor injury

System Safety

- System safety is determined by the residual risk of the boundary hazards exported to its environment. The key inputs are
    - Safety Targets
    - Hazard Log
    - Interface Hazard Analysis
    - System Hazard Analysis
    - A SIL may be determined for the whole system provided the subsystems has definite SIL levels
  - System safety is required to be demonstrated by providing an specific application Engineering safety case.

Product safety

- Product safety is controlled by the product approval processes. The main inputs are
  - SIL assessment
  - Hazard Log
  - Evidence from Trials and Testing
  - A generic product safety case (for a specific application)

Safety Targets

Safety Targets are determined from the most restrictive of

- HSE directive. HSE directive define quantitative allowable passenger risk and staff risk.
- Railway group targets
- Railway targets set by the customer
- An apportionment of the overall risk to the section of railway being changed to be done and the risk need to be calculated. This target will determine the upper limits of tolerability.
- If the total risk comes in between upper limit of tolerability and lower limit of tolerability then ALARP is required to be demonstrated.

Likelihood-severity matrix

	Insignificant	Marginal	Critical	Catastrophic
Frequent	Undesirable	**Intolerable**	**Intolerable**	**Intolerable**
Probable	Undesirable	Undesirable	Undesirable	**Intolerable**
Occasional	Tolerable	Undesirable	Undesirable	Undesirable
Remote	Tolerable	Tolerable	Tolerable	Undesirable
Improbable	Acceptable	Tolerable	Tolerable	Tolerable
Incredible	Acceptable	Acceptable	Acceptable	Tolerable

Probability of Hazard occurring

Note: it is recommended to split the frequency or likelihood into two components:

- the frequency or likelihood of a hazard occurring;
- the likelihood of an accident occurring given that the hazard has occurred.

This can remove some excessive conservatism for hazards that are unlikely to lead to a hazard but, of course, the tables become three-dimensional and more difficult to handle.

ALARP (As Low As Reasonably Practicable)

Add sub-title

- Design is compliant with applicable standards
- the standards cover your situation.
- the equipment is being used as intended;
- No feasible option to lower the risk. In quantitative assessment Value of Preventing Fatality (VPF) used. In UK it is 1.4 million pounds.

Mitigations and Control

Hazard analysis is undertaken with the domain experts to identify mitigations and controls to reduce the risk.

The mitigations are set in the following order of preference

1. Safety features of the product/system
2. Operational procedures
3. Additional barriers to contain the hazard.

Safety requirements

Safety requirements may specify:

- actions to control risk;
- specific functions or features of a railway product or a part of the railway;
- features of maintenance or operation practices;
- features of design and build processes; and
- tolerances within which something must be maintained.

Operation & Support Hazard Analysis

- Generally done at after the development phase.
- Objective is to minimise hazards arising from human errors
- Procedures are analysed for deviations at each step to identify any hazards
- Operational controls will be identified as mitigations to the hazards identified.
- O&SHA is conducted in the detailed design phase mostly part of the HAZOP study and before commissioning phase.
- “Day in the Life” approach is mostly employed to identify any operability hazards

Overview of CENELEC Standards

- CENELEC standards are mandatory on rail jobs in UK & Europe.
- CENELEC Stanadards are process standards. The key standards are
- CENELEC 50126
- CENELEC 50126 -1
- CENELEC 50126-2
- CENELEC 50128
- CENELEC 50129

CENELEC 50126

50126 Basic Requirements and generic process

The original process RAMS standard is maintained. The essential deliverables are

- SIL assessment
- RAMS specification which contain RAM and safety targets
- RAM and Safety plans, Hazard Log
- RAM Analysis, Preliminary Hazard Analysis reports
- RAM demonstration, FRACAS, System Hazard Analysis reports
- Engineering Safety Case

EN50126-1

Guide to the application of EN 50126-1 for safety

- A European Yellow Book equivalent
- Explain risk assessment process in detail
- Describes the Safety and RAM Techniques FTA, FMECA, ETA, Hazard checklists
- Safety Case structure

CENELEC 50126-2

- Rolling stock safety standard
- Provides guideline on the safety processes to be applied

CENELEC 50128

Software for railway control and protection Systems

- Qualitative software safety integrity levels
- Safety critical software development has its own specific set of documentation in accordance with the software system lifecycle
- Specific set of deliverables with respect to the software development life cycle is listed
- A separate independent assessor is required
- Application data is also covered under this standard.

CENELEC 50129

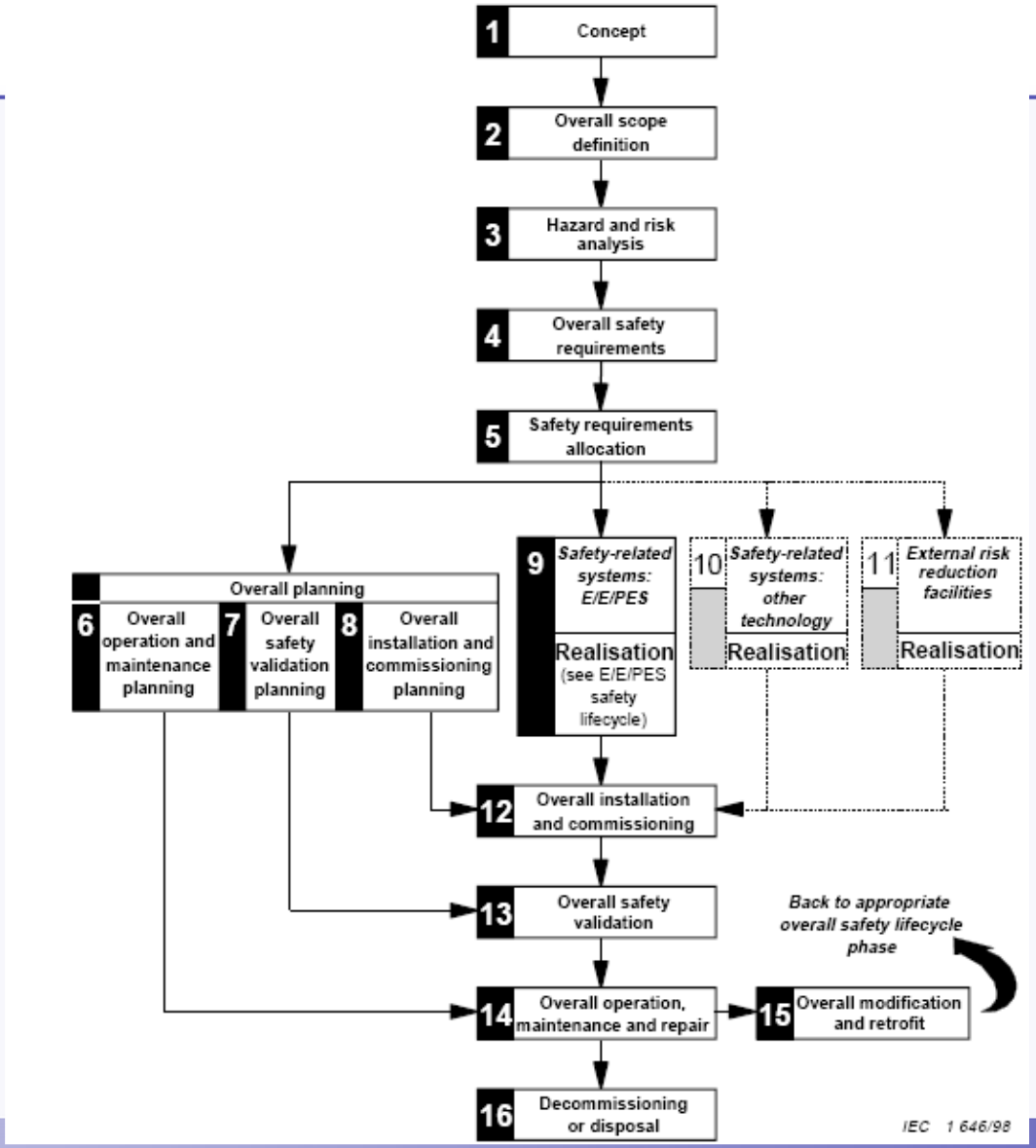
Safety Case

- Structure,
- document template
- Description of each section
- Appendices for Technical safety report

Safety Processes

- Safety Integrity levels
- Failure mode identification

Safety Life Cycle


1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal
IEC 1 646/98

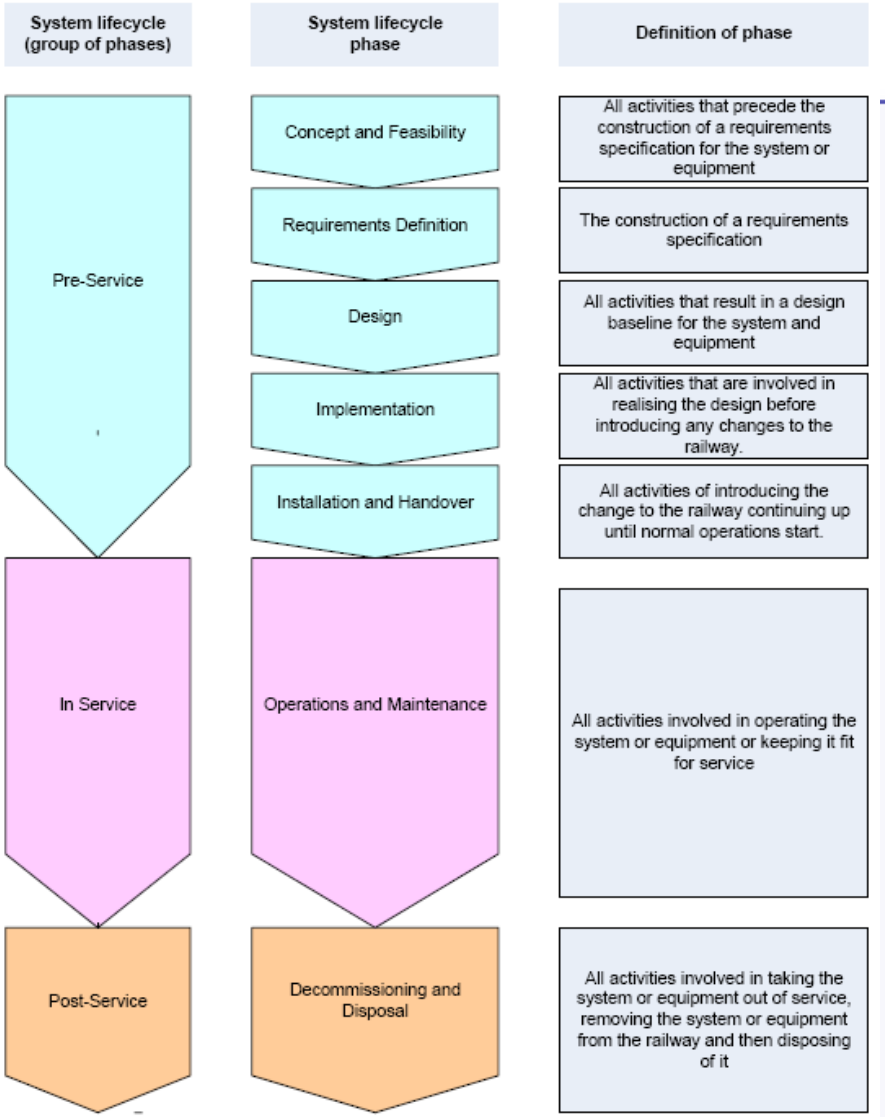


Figure 2-3 The System Lifecycle

Safety Documentation

Engineering Safety Plan

See yellow book page 276.

The main points are

- Risk based approach to be taken
- To be agreed with customer as well as ISA
- To be reviewed and updated during the course of the project.

Preliminary Hazard Analysis (PHA) Report

No standard format available. The following points to be covered

Introduction

- System description specifically on boundaries
- Methodology
- Hazard table shall include at least
  - Checklist items
  - deviation
  - Hazards
  - Causes
  - Unmitigated risk
  - Mitigations and control
  - Safety requirements
- **PHA once done is not changed during the course of project unless the scope of the project changes.**

HAZOP/HAZID report

No fixed format available. The report should contain

- System functional description and functional architecture
- HAZOP methodology
- Hazard table should contain
  - Design intention/Operational parameter
  - Keyword
  - Deviation
  - Hazard
  - Causes
  - Unmitigated Risk
  - Mitigations
  - Safety requirements
  - HAZOP is complimented with O&SHA

Interface Hazard Analysis report

- IHA focus on system interactions with the environment.
- IHA should identify transfer of control with neighbouring signalling system, interaction with other suppliers equipment.
- System functional description and functional architecture
- HAZOP methodology
- Hazard table should contain
  - Interface
  - Interaction
  - Keyword
  - Deviation
  - Hazard and other hazard log parameters

System Hazard Analysis report

- SHA is the main supporting document for safety case.
- Residual risk assessment of the system by establishing residual risks of the system boundary hazards.
- ALARP assessment of the system boundary hazards.

The document should contain

- System configuration
- Boundary hazards,
- Safety requirement compliance
- Residual risk estimate,
- Options analysis,
- ALARP assessment

Engineering Safety Cases

Engineering Safety Cases

Engineering safety cases are mandatory document to be made in accordance with EN50129 supported by an ISA report (preferred) submitted to Safety authority. This submission is required with progressive evidence on

- End of Design Phase
- Beginning of Testing Phase
- Beginning of Operational phase

These submissions are required for commissioning new and novel system. For a conventional signalling system one safety case can present evidence for all the phases.

Engineering safety case structure

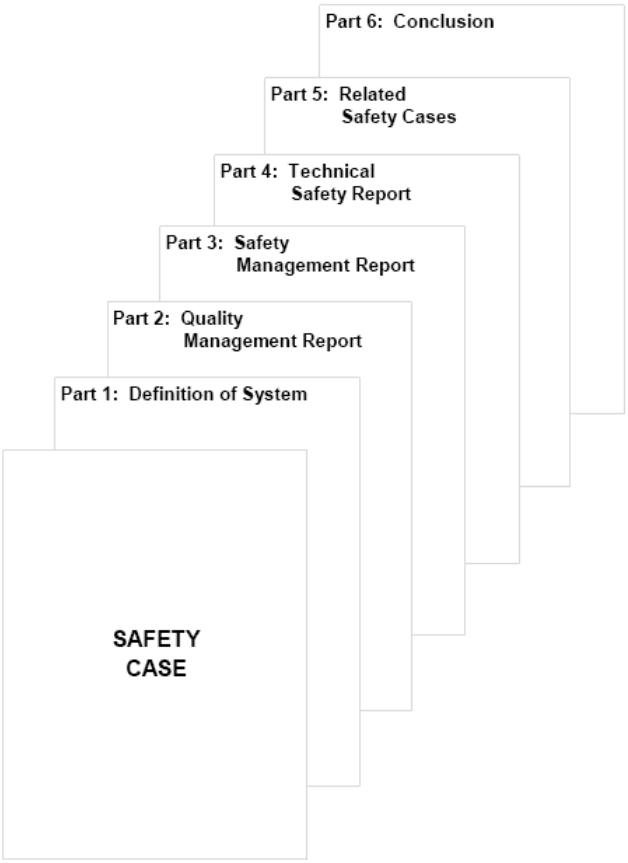


Figure 3 – Structure of Safety Case

Definition of the system

General issues

- Boundaries are not well defined.
- Interface issues at the boundaries are not resolved
- Transferred hazards are not managed
- Operating and maintenance procedures not developed.
- Necessary consultation with the stake holders are not done correctly.
- WEE and RohS directives (Environmental directives not fulfilled)

Quality Management report

Generally restricted to ISO audits. These audits may not cover all project activities.

Non conformances, Observations not addressed properly.

Safety Management report

Main issues are

Hazards not satisfactorily mitigated.

Hazards transferred to the suppliers are not managed.

Safety requirement compliance evidences are not satisfactory.

Hazard data configuration is not properly managed.

Hazard mitigation evidences are not properly managed.

Technical safety report

Main issues are

- SIL assessment not properly done
- Tolerability criteria not consistent with industry targets
- Options analysis and evaluation not done in the ALARP assessment
- Non compliances to standards are not managed properly.
- Residual risk not assessed correctly

Related safety cases

Main issues here are

Related safety cases are not properly managed.

Dependencies of the main safety case not properly established.

Engineering Safety Case-Design

Design Compliance

This present the case that the design

- fulfil safety requirements on design,
- compliant with standards subjected to concessions, design produced by competent people
- using approved products

Engineering Safety Case-testing

This safety case present the case that

- Safety of the operational railway is not jeopardised when taken for testing, handover.
- Factory acceptance Tests are complete and passed
- Installation is completed.
- Installation tests and other static tests are passed.
- Test procedures, Acceptance criteria are in place.

Engineering Safety Case commissioning

This safety case present the case that

- O&SHA is completed and all safety issues coming from O&SHA has been mitigated.
- The system is ready for operation.
- The system has passed all safety testing.

Independent Safety Assessment

Independent Safety Assessment (ISA)

Independent Safety Assessment is regarded as good practice and therefore provides additional protection against negligence.

ISA's professional duty is to be independent. Customers and projects pay for the Independent Safety Assessment activity but should not direct or influence the ISA in any way which might compromise the ISA's independence or the robustness of the assessment.

The ISA is professionally bound not to give advice to those projects which it is assessing. The ISA can only offer guidance where it is general and non-specific.

Levels of independence of ISA at each SIL

MINIMUM LEVEL OF INDEPENDENCE	SAFETY INTEGRITY LEVEL			
	1	2	3	4
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	NR
Independent Organisation	-	-	HR	HR

Qualifications of Safety Auditor/Assessor

Qualifications for Safety Assessor	Qualifications for Safety Auditor
Chartered Engineer status or equivalent in an engineering or scientific discipline relevant to the system or equipment;	
prior experience as a Safety Assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;	prior experience as a Safety Auditor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
demonstrable application domain experience;	
experience of process assurance (for instance quality or Safety Audits);	experience of process assurance (for instance, quality or Safety Audits);
familiarity with external safety standards and procedures;	familiarity with external safety standards and procedures;
familiarity with the legal and safety regulatory framework within which UK railways operate;	familiarity with the legal and safety regulatory framework within which UK railways operate
training in ESM.	training in ESM.

Safety responsibilities of various roles

- Customer (initiates the requirement for change, then operates or uses the results of a change);
- Project (engineers the change and controls the risk);
- ISA (reviews the change and assures that the risk associated with the change is as low as reasonably practicable (ALARP));
- Safety Authority (accepts the change and its associated risk);
- Notified Body (verifies that change conforms to applicable standards).

Interactions between various roles

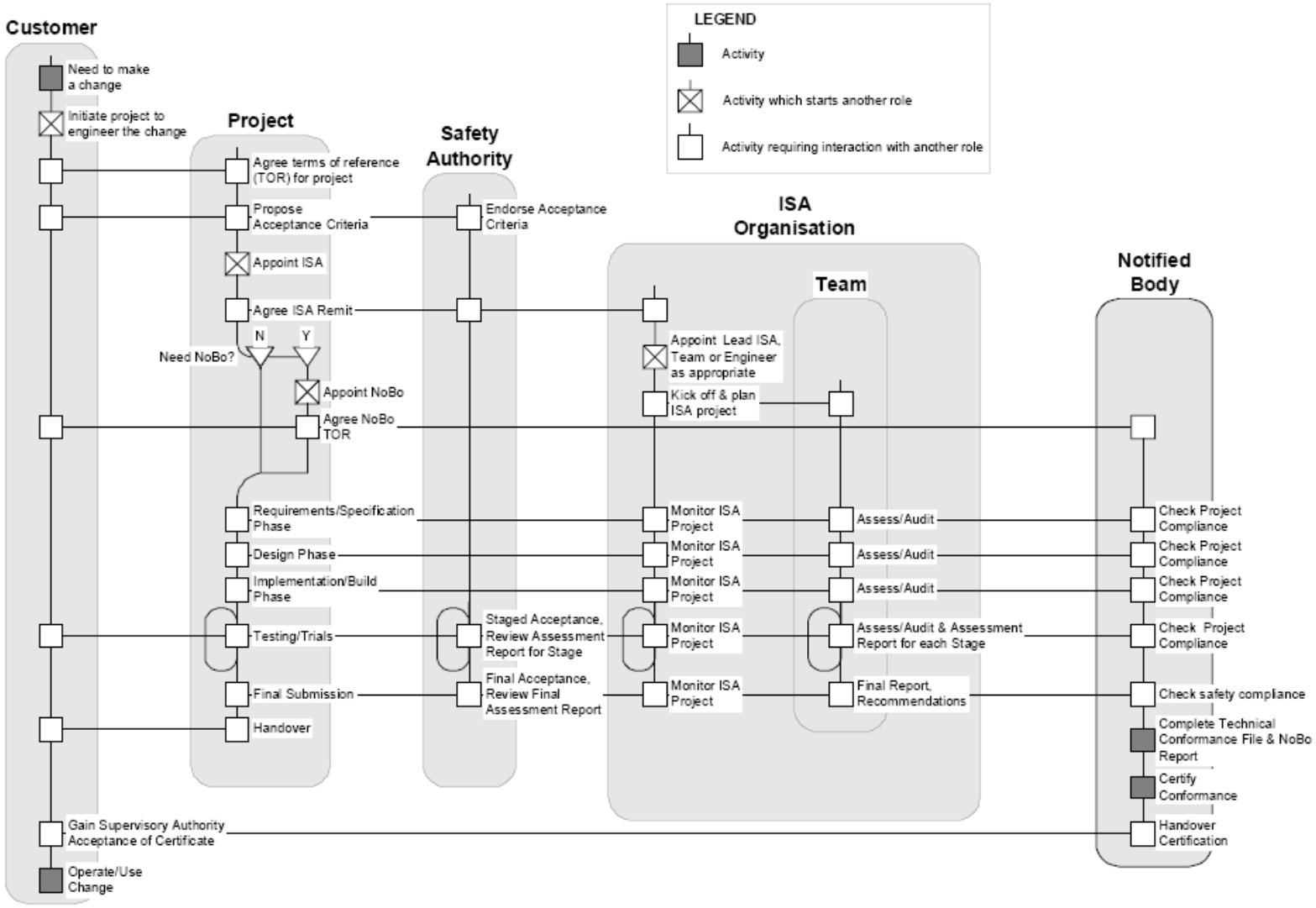


Figure 1: Illustrative Interactions Between Roles (for a Generic Change Project)

ROLES IN EACH SYSTEM LIFECYCLE PHASE

	CONCEPT & FEASSIBILITY	REQUIREMENTS DEFINITION	DESIGN & IMPLEMENTATION	INSTALLATION & HANDOVER	OPERATIONS & MAINTENANCE	DECOMMISSIONING & DISPOSAL
Customer Project	Develop ISA Remit ISA Selection Seek approval of remit	Maintain Remit Handle ISA Observations Handle ISA Reports Liase with Safety Authority	Maintain Remit Handle ISA Observations Handle ISA Reports Liase with Safety Authority	Maintain Remit Handle ISA Observations Handle ISA Reports Liase with Safety Authority Execute Trials	Close all open ISA Observations Seek and obtain Safety Authority Approval	Disposal in accordance with accepted provisions of the safety case
ISA Organisation	Demonstrate Competence, Independence and Commercial Confidence Respond to remit, provide feedback	Monitor Competence, Independence and Commercial Confidence Interface with NoBo	Monitor Competence, Independence and Commercial Confidence Interface with NoBo	Monitor Competence, Independence and Commercial Confidence Interface with NoBo	Monitor handover on completion	
ISA Team ISA Engineer	Technical Assessment Planning Competent Staffing Schedule: Tasks & Timescales	Use a risk-based approach Raise observations Perform Assessment Audit Activities	Use a risk-based approach Raise observations Perform Assessment Audit Activities Liaise with Safety Authority	Use a risk-based approach Raise observations Perform Assessment Audit Activities Liaise with Safety Authority Assess trial results	Produce final ISA report Make representation to Safety Authority Complete & handover	
Safety Authority	Provide means of recognising or approving ISAs as competent Approve ISA selection Refine/Approve ISA Remit	Review ISA output Manage Projects IPR Mentor Project and ISA	Review ISA output Manage Projects IPR Mentor Project and ISA	Review ISA output Manage Projects IPR Mentor Project and ISA Monitor trials	Review Project Safety Case and ISA Assessment Report then Endorse/Accept Project's change	

Safety Review

Independent Safety Review Panel

Independent safety review panel (ISRP) consists of discipline experts of Signalling/ Rolling Stock/ Power, Safety and RAM, Human factors, HSEQ rep etc.

- ISRP is the represents Railway safety board
- Endorsement of ISRP grants permission to test/commission
- ISRP has clear Terms of Reference, review procedures.
- All submissions from supplier/integrator/operator for bringing change to the railways shall be approved by ISRP.
- Level of review depends on the risk brought in by the change.

Implementation Tips:

- Start safety engineering early
- Treat safety engineering as an integral part of engineering
- Use a qualitative assessment to quickly home in on the main issues
- Scale efforts according to the relative level of risk; no absolute measures
- Incremental process; stepwise refinement
- Aim to produce a logical and compelling case for safety, one that clearly separates the safety argument from any safety evidence
- Work with the ISA and Safety Authority to make the case; do not rely on them as a safety net

RAM Assurance

RAM performance related with safety shall be treated as safety requirements and should be included as standard.RAM performance related to business targets shall be included as part of the contract. RAM activities in each project phases are outlined below.

- Invitation To Tender
  - RAM Targets
  - RAM requirements
- Concept Design
  - RAM Plan
  - Preliminary RAM report

RAM Assurance

- Detailed design
  - RAM Analysis
    - minimise single point failures;
    - CCF analysis
    - graceful degradation
    - RAM prediction
  - RAM modelling
    - Analysis of Impact on service due to failures
    - Optimisation of maintenance and spares strategy

RAM Assurance

- Testing
  - RAM demonstration i
  - Reliability Growth
  - DRACAS
- Post commissioning
  - RAM Targets in-service compliance
  - FRACAS

Intellex RAMS Assurance Ltd.

Company house Regn

www.intellexrams.co.uk

Contact info@intellexrams.co.uk

Ph:-0044-(0)-7984456146