RAMS Systems Assurance for Railways

By George Ardavanis, PhD

Keywords: *reliability, availability, maintainability, safety (RAMS), design, build, operation and maintenance (DBOM), operation and maintenance (O&M), mean time between failures (MTBF), mean time to repair (MTTR), quantitative risk assessment (QRA), root cause analysis (RCA), failure recording and corrective action system (FRACAS), failure mode effects and criticality analysis (FMECA), line replaceable unit (LRU), factory acceptance tests (FAT), corrective maintenance cycle (CMC), reliability and maintainability (R&M), RAMS demonstration plan (RDP)*

Introduction

RAMS systems assurance is a framework for railway transit authorities and their contractors to ensure that railway systems have been designed, constructed and operated according to all critical factors related to safety, reliability, maintainability, and availability.
Reliability, availability and maintainability (RAM) are those qualitative and quantitative indicators of the degree that the railways' equipment and systems can be available to function efficiently.

1.0 RAMS systems assurance approach

The RAMS systems assurance is a holistic management approach which can:

- Provide analytical techniques as a metric with regards to performance
- Be used as a management tool via which one can coordinate and assure the whole DBOM cycle

RAMS systems assurance must be implemented from the beginning of the project cycle to achieve the best project results. As a project progresses it becomes very hard to introduce RAMS systems assurance tools to successfully implement critical design changes.

2.0 RAMS systems assurance project cycle

During conceptual, preliminary, and final design, as well during construction the engineering, operation and maintenance departments should fully participate in the RAMS systems assurance in order to review and discuss the existing design, the O&M plan and targets, the O&M prerequisites, and identify potential hazards to public and railway personnel.

Design changes or modifications may be required during a project cycle for a variety of reasons. Any design change or modification should be notified, recorded and reviewed by the engineering and O&M departments.

Analysis methodologies in RAMS systems assurance can assist railway engineers to determine which design changes or design modifications are proper for given circumstances. The RAMS systems assurance process identifies potential hazards introduced by specific design changes. If multiple design options are available the RAMS systems assurance management process can identify potential hazards of each design option, provide risk ranking to each hazard, and control each risk accordingly. If the risk rankings for alternative designs are similar, cost/benefit analysis can be performed to identify implementation costs for each design modification and compare risks and benefits introduced by each design modification. This assists the client, the contractor and the project engineer to decide which design is more cost effective and/or less risky to the agency. Moreover, cost/benefit analysis can be performed to compare the mitigation measure implementation costs with the associated benefits to the systems.

2.1 Planning and preliminary design

During planning stage no specific RAMS activities are performed. Nevertheless usual RAMS criteria will be incorporated into the selection of the suitable rail system technologies (standard design rules of redundancy, etc.)

During preliminary design the RAMS objectives (e.g. MTBF, system level service availability requirement, system service delays requirement, maintainability requirement, etc.) will be apportioned to the different civil works and electromechanical subsystems, and to the O&M activities, according to the mission profile analysis and corresponding simulations.

At the end of the preliminary design phase the contractors should prepare a “preliminary reliability report” setting out the expected reliability figures for each of the systems and individual items of equipment.

2.2 Final design and construction

During the pre-final design stage the design of the system proceeds to a point where the final design options are presented before being frozen. During pre-final stage, the entities in charge of RAMS activities at the subsystem level develop the associated RAMS performance forecasts.

During the final design stage RAMS activity consists in integration and theoretical validation of the overall RAMS performance forecast at the system level.

RAMS systems assurance tools such as MTBF, and MTTR of components, equipment and systems can assist the engineering department to determine which designs and components provide more reliable and available service to the public. System safety and assurance department can also utilize the MTBF and MTTR data to propose improvement to maintenance plans for the railway products and services.

2.3 Manufacturing, installation, integration

During this stage there will be a follow-up of the RAMS studies according to the changes, and the generation of the RAMS demonstration tests plans.

2.4 Testing and commissioning

The department responsible for testing and commissioning should collect all product and system performance data and work with the RAMS systems assurance management in order to analyze the data. During testing and commissioning operational and maintenance targets should be tested as products and systems operating in the design environment respectively. Specifically, performance compliance of the installed subsystems is verified at the individual level and at the integrated level to commission the system. RAMS performance monitoring is initiated, and maintainability tests may be performed.

In case of product and system failures, that are not identified during the design phases or do not meet any O&M targets, then it is suggested to perform RCA in order to identify the cause of failure.

2.5 O&M

Upon completion of the test and commissioning stage of a railway project, revenue operation may proceed. At this stage, RAMS activity consists in demonstrating that the overall RAMS performance forecasts of the railway system are met, through a RAMS demonstration test.

Operations can review the human machine interface design to improve usability, while maintenance personnel can review the design for such items as easy to access lowest replacement units, diagnostics and identification of the root causes of the failures and reduction of time to perform maintenance on the systems.

During system operations or under revenue service, RAMS systems assurance management should work with O&M departments to monitor the performance of products and systems. O&M departments should provide O&M data to RAMS systems assurance management for analysis. These analyses will assist to prevent any unpredictable hazards or failures and ensure that products and systems meet reliability, availability, maintainability, and safety targets predicted during the design phase.
If any incidents will occur during operations, then O&M departments should work closely with engineering and the RAMS systems assurance departments to perform safety analysis and identify the cause of the incidents and any required design modifications.

2.6 RAMS systems assurance services

Below there is a summary of RAMS systems assurance activities by project stage. These studies may be required subject to the "railway authority instruction".

	FS	D	C	T&C	DLP
Preliminary hazard analysis	O	I/O			
Preliminary RAM analysis	O	I/O			
System Assurance Plan		O	O		
Hazard management: hazard analysis, review, control, and monitoring		O	U	U	U
Functional block diagram		O	U	U	U
Failure modes, effects, and criticality analysis		O	U	U	U
Reliability block diagram		O	U	U	U
RAM modeling, allocations, and predictions		O	U	U	U
Fault tree analysis		O	U	U	U
Event tree analysis		O	U	U	U
Safety integrity level (SIL) analysis for safety related systems		O	U	U	U
System compliance audit		A	A	A	A
RAM performance demonstration				A	A
Failure reporting and corrective action system			A	A	A

Where:

FS = Feasibility Study, D = Design and configuration, C = Construction and installation, T&C = Testing & commissioning, DLP = Defects liability period, A = Activity, I = Input to phase, O = Output from phase, U = Updated during phase

2.7 Tests and follow up of RAMS parameters

The purpose of these tasks is to verify that the RAM requirements will be achieved in revenue service. This task will be performed by appropriate tests and/or follow up of the system level RAMS parameters.
The performance of the railway system will be demonstrated on-site during the pre-revenue service running period.
The RAM demonstration program and management will be presented in the RAMS demonstration plan (RDP) to be issued at end of the detailed design phase. This RDP plan will address, regarding the RAM parameters to be followed:

- The acceptance criteria
- The organization to be implemented
- The methods and tools to be used
- The tests report to be emitted

The RDP will be supported by a failure reporting and corrective action system methodology, and specific reports will be emitted in addition of the final report. They are:

- Periodic report allowing to give status of the reached and projected values (growth),
- Specific reports in case of unacceptable values of parameters regarding the projected value.

All test documentation shall be subject to review in accordance with the requirements and procedures defined in the contract.
The criteria for passing the RAM Demonstration will be based upon:
• The mean RAM parameter performance calculated over the period of demonstration,
• A confidence level to be defined.

The method and a precise definition of the pass criteria will be presented in the Test Plans and submitted to the Employer for approval. The DBOM Contractor will be involved in the discussions and in the decision making concerning the failures observed during the on-site demonstration period, and its agreement will be required, in particular for the attribution of failure responsibility.

3.0 RAMS system assurance railway breakdown

For the RAMS systems assurance studies, the following breakdown shall be used:

- Rolling stock
- Train Control System
- Railway track
- Power supply system
- Civil works and infrastructure
- Operations management
- Maintenance management
- Communication (internal and passengers)

4.0 RAMS systems assurance requirements

The expected RAMS requirements for the various equipment and systems should be with the client prior to invitation to tender. The inability to perform any required function, the occurrence of unexpected action or the degradation of performance below the specifications should be considered a failure. Specifically, the RAMS requirements are identified in the areas of:

- **Quantitative system RAMS contractual requirements** – The quantitative RAM system and subsystems will be generated during the preliminary engineering, when the alignment and composition of the railway system are known. They may be expressed with the following criteria:
  - MTBF
  - System level service availability requirement
  - System service delays requirements
  - Extent of delay
  - Maintainability requirement, etc.
- **RAMS requirements on methodology and organization** – The contractual documents specifies as well how the RAMS tasks should be organized and identifies methodologies that are allowed to conduct the work

4.1 Applicable standards

The applicable standards should be set-down in the tender documentation and specifications.

4.2 FMECA analysis

The contractors should perform FMECA analysis in accordance with the process requirements set out in the tender documentation and technical specification.

4.3 FRACAS

The contractors should have clear instructions set-out in the tender documentation and specification to fulfil this requirement. FRACAS will be established starting by a FRACAS plan issued during the final design phase. The FRACAS will be maintained throughout the various phases including operation.

5.0 RAMS systems assurance activities

5.1 RAMS systems assurance activities during design phase

Normally RAMS systems assurance activities would comply with the following:

- Cenelec EN50126:1999 – Railway applications – The specification and demonstration for RAMS
- Cenelec EN50128:2001 – Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems
- Cenelec EN50129:2003 – Railway applications – Communications, signalling and processing systems – electronic systems for signalling

During the design phase of a railway project, the following activities should be carried out by the contractors:

- **Reliability activities**
  - **Reliability assessment** – Obtain MTBF figures from the suppliers and where necessary ask for the FMECA carried out for the systems
  - **Corrective actions** – If an item fails to meet the specified reliability requirements, the supplier should be alerted and the taken the necessary steps to ensure that the design of the equipment is modified such that the required MTBF figures can be reliably achieved
  - **Preliminary reliability report** – At the end of the design phase the contractors should prepare a preliminary reliability report setting-out the expected reliability figures for each of the systems and individual items of equipment

- **Maintainability activities** – before the maintainability of a railway systems could be estimated, the following factors need to be taken into consideration:
    - **Maintenance** – constitutes the act of diagnosing and repairing, or preventing system failures and can be divided into preventive maintenance and corrective maintenance
    - **Maintenance policy** – refers to the means by which the RAMS engineer will identify the maintenance tasks and maintenance logistics. Maintenance tasks (both corrective and preventive) should be undertaken as part of a 3-stage process that can be defined as: (1) 1^{st} line maintenance, (2) 2^{nd} line maintenance, and (3) 3^{rd} line of maintenance. Additionally, the list of basic logistics items (tools, spare parts, test equipment, consumables and manpower) necessary to maintain the various equipment and systems should be provided by the contractors in a maintenance plan which should be the subject of a separate submission
    - **Maintainability** – constitutes an inherent design characteristic dealing with the ease, accuracy, safety and economy in the performance of maintenance functions. The maintainability parameter that needs to be measured should be the "time required to perform maintenance tasks", quantified in terms of MTTR to full normal operation following a failure. For railway contracts, MTTR should be considered to commence from when the maintenance personnel arrive on-site and conclude when the system is restored to operation
    - **Achieving maintainability** – In order to ensure that the equipment and systems that have been supplied are capable of being restored to service in the minimum times possible, an analysis to determine the MTTR for those systems that may contribute to the in-service availability for the railway should be carried out as soon as the configuration of each of the systems is finalised. Thus the MTTR for each of the railway systems should be determined as shown in the equation below:

      $MTTR = \frac{\Sigma(\lambda i)(LRUi)}{\Sigma(\lambda i)}$, where λ is the failure rate (1/MTBF) of each individual (*i*th) LRU

- **Availability activities** – Is the ability of a product to be in a state to perform a required function under given conditions at a given instant in time or over a given time interval assuming that the required external resources are provided (EN 51021).

  $\text{Availability} = \frac{\text{MTBF}}{(\text{MTBF+MTTR})}$, where MTTR = 1 hour

    - **Block diagrams** – They show the configuration of each system should be produced, progressively expanded to show the constituent part of each system down to LRU level
    - **Fault tree analysis** – The reliability characteristics of the equipment should be calculated using Boolean probability theory or a homogeneous Markovian process in accordance with IEC 61205 (fault tree analysis) with the aid of a proprietary program such as "fault tree plus" or "zuzim" and the output should be in the form of a "fault tree" diagram
    - **Preliminary availability report** – Using the calculation methods described above, the availability of all the major systems should be calculated and a preliminary report should be prepared by the contractors

- **FRACAS** – The contractors should institute a FRACAS, which should be a closed-loop feedback path by which failures of both hardware and software data are collected, recorded, analyzed, and corrected. The aim of the system should be to aid design, to identify corrective action tasks and to evaluate test results, in order to provide confidence in the results of the analysis activities and in the correct operation of the equipment features. Full details of the FRACAS process should be set out in a FRACAS management plan to be prepared by the contractors
- **Establishment of a FRACAS review committee** – In conjunction with the project engineer the contractors should establish a FRACAS review committee to manage how RAMS corrective actions are to be identified, assessed and recorded

5.2 RAMS systems assurance activities during construction phase

During the construction phase of a railway project, the following activities should be carried out by the contractors:

- **Reliability tests** – With regards to the confirmation of the reliability figures, given by the system suppliers, will be the responsibility of the contractors to organize any reliability tests required during the FAT for various systems
- **Maintainability demonstrations** – With regards to the confirmation of the CMC time for any item of equipment, it will be the responsibility of the contractors to organise any maintainability demonstrations required during the FAT for the various systems

5.3 RAMS systems assurance activities during warranty monitoring phase

5.3.1 FRACAS review

During the warranty monitoring phase of the project, the following activities should be carried out by the contractors should keep full records of any failures and the corrective actions taken to restore the equipment to full service and input the record data into the FRACAS for the review committee to evaluate

5.3.2 Final reliability report

At the end of the warranty monitoring phase, a final reliability report should be prepared by the contractors confirming the in-service reliability of the equipment and systems.

5.3.3 Final maintainability report

At the end of the warranty monitoring phase, a final reliability report should be prepared by the contractors confirming the in-service maintainability of the railway equipment and systems

6.0 RAMS tasks

6.1 Reliability tasks

Reliability tasks are initiated as early as possible in the design and must be updated as the design goes on. These tasks allow achieving 3 different goals:

- **Perform an initial apportionment and modelling of the overall reliability goals.** This is carried out for each subsystem during the preliminary design period, so that each of them can be studied separately
- **Achieve the reliability prediction of subsystems.** The purpose of the reliability prediction is to make an early evaluation of the reliability level that subsystems are expected to reach. The

prediction can be done as soon as the design is known. It is then possible to compare it to the target and carry out appropriate design improvement actions until the reliability goal is reached

- **Achieve a design that responds to the reliability goals.** Through reliability analysis, the critical areas where additional design efforts must be undertaken to eliminate the occurrence of certain potential failures that might affect the reliability of subsystems are identified.

To achieve these goals, the following tasks should be implemented throughout the design stages of the railway project:

- **Preliminary design**
  - Mission profile analysis
  - Subsystems description
  - Criticality analysis
  - Reliability modelling and apportionment
- **Pre-final design**
  - Prediction of intrinsic reliability
  - Detailed failure mode effects analysis
- **Final design**
  - Consolidating analysis performed at the subsystems levels
  - Spare parts analysis

6.2 Maintainability tasks

Maintainability contributes to system availability and is also the main cost driver during the operational phase of a system. For this reason, maintainability tasks are initiated at the early stage of the design and are regularly updated as the design progresses. These tasks have the following 3 objectives:

- Perform an apportionment of the maintainability goals at subsystem level
- Achieve a design that complies with maintainability requirements by first identifying areas that are critical in terms of maintainability and then eliminating any potential problem that might affect the maintainability of subsystems
- Achieve the maintainability prediction of each subsystem by conducting an evaluation of the maintainability level that subsystems are expected to reach

6.3 Availability tasks

As a basic principle the “availability” performance of a system depends on its “reliability” and “maintainability”. As a consequence, the availability tasks consist in a consolidating analysis at system level of the reliability and the maintainability tasks results.

The purpose of this consolidation is to assess, on the basis of the actual design, the level of the availability at system level and verify that the contractual system availability objectives are reached.

The analysis is based on:

• Results of the subsystems reliability tasks
• Results of the subsystems maintainability tasks
• RAM apportioned / predicted targets

This tasks can be done by RAMS techniques and tools such as the reliability block diagrams, fault tree analysis, FMECA, etc. This consolidation tasks can involve an (up-down) iteration process, leading to update some of the reliability and / or maintainability tasks, in order to reach the defined targets for the system availability.

In addition of this process, the field demonstration will be detailed further in the project life cycle, through the RAMS demonstration plan.

7.0 System safety

All failures adversely affect system reliability, whilst only some failures will have an adverse effect on safety. To realise safe, dependable railway systems with regards to all those factors that affect reliability, availability and maintainability, need to be identified and managed. The relationship between reliability, availability, maintainability and safety is shown in Figure 1.

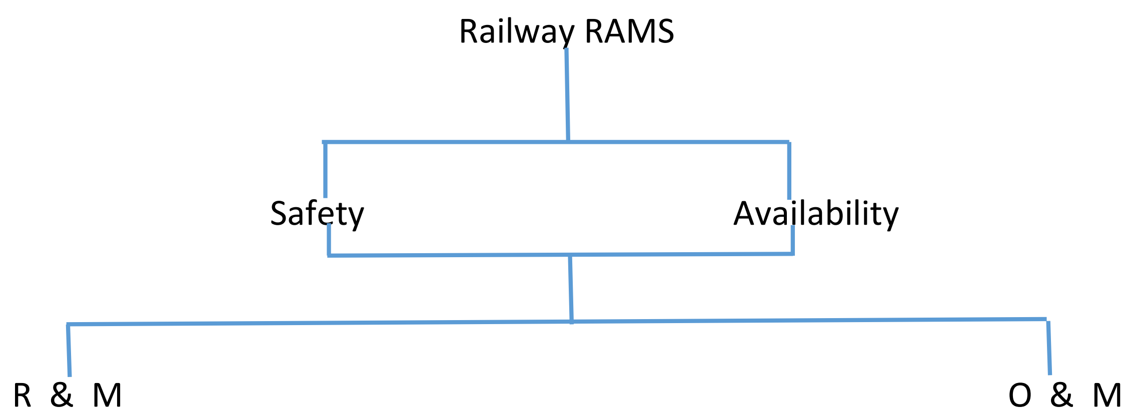

Figure 1. Inter-relations of railway RAMS elements

Safety and availability are interlinked in the sense that a weakness in either or mismanagement of conflicts between safety and availability requirements may prevent achievement of a dependable system. The inter-linking of railway RAMS elements, reliability, availability, maintainability and safety is shown in Figure 2.

Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment.

Any reliability errors which are disclosed during testing. For example, see Figure 2, the yellow reliability in the bottom will cause a yellow availability in the middle, which again will cause a yellow top level railway RAMS. Since we have a green maintainability in the bottom, it might be possible to increase the "maintenance " work for the yellow "reliability", so we receive a green "availability ", which again will cause a green top level "railway RAMS". See Figure 3. This is called controlling RAMS.

A railway system safety is based on:

- Risk (hazard) identification. According to EN 50126 part 2 hazard is defined as "a condition that could lead to an accident)
- Safety related (reliability, availability)

- Maintainability of safety related elements of the system
- Operation of safety related parts of the system
- Maintenance of safety related parts of the system
- Functionality of safety related parts of the system

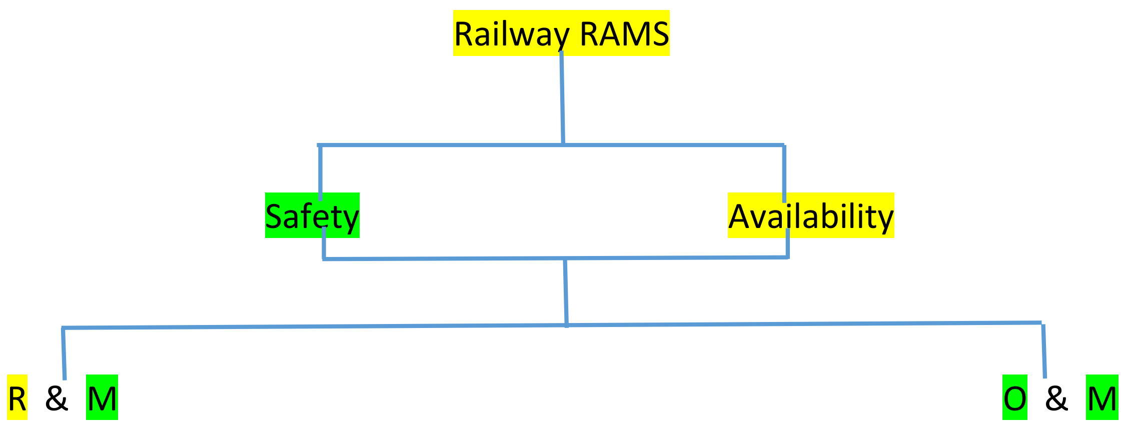

Figure 2. Impact of disclosed reliability error during railway testing

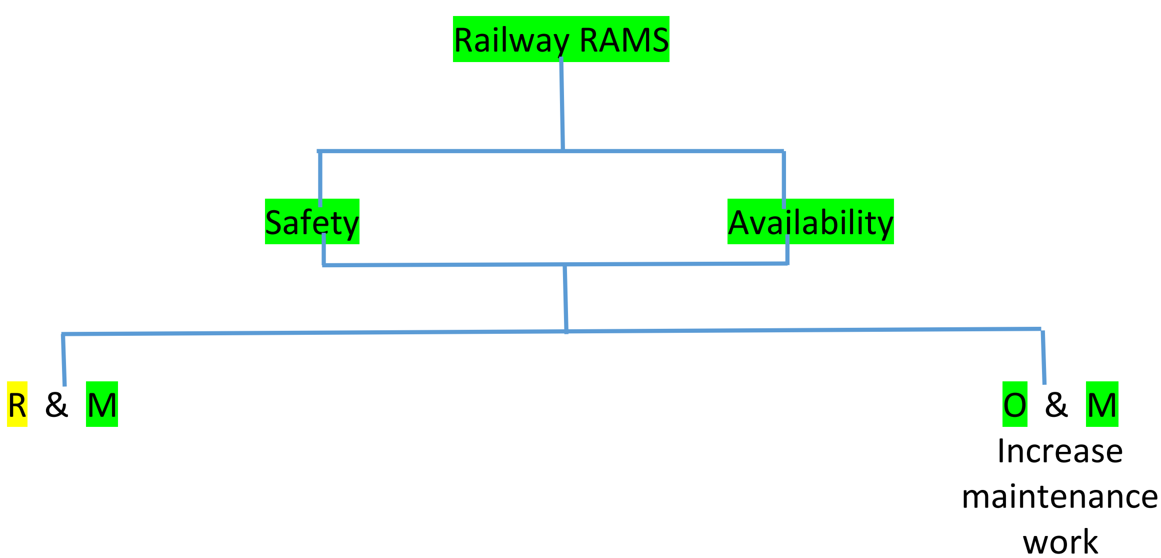

Figure 3. Controlling RAMS by increasing maintenance work

7.1 Railway system safety plan

The objective of a railway overall system safety plan should:

- Define responsibility for the management of the system safety related activities
- Define the risk categories
- Define the safety related activities that will be performed
- Determine the sequence of events for safety activities
- Describe the approach and the methods of risk analysis to be performed
- Ensure that all safety related activities are implemented within the overall guidance framework for managing reliability, availability, maintainability, and safety set-out in EN 50126 parts 1 and 2

7.2 Railway safety case

A railway safety case should describes the arrangements for safety management for an organization which manages infrastructure or operates trains or stations and any organization which manages infrastructures or operates trains is normally obligated to write a railway safety case and have it accepted/put into practice before starting operations. The operator must then follow their safety case.

8.0 RAMS systems assurance plan

It covers the RAMS systems assurance activities and management to be implemented during the whole life cycle of the railway project. Specifically, it includes the following:

- Railway organization and the associated responsibilities in terms of RAMS, as well as inside the general project organization
- Railway safety policy and the RAM concept on which are based the RAMS demonstration
- Activities that are implemented to evaluate, verify and validate the RAMS through each phase of the whole life cycle
- Presentation of the analysis to be performed
- List of RAMS deliverables associated to the milestones of the project

9.0 RAMS systems assurance modelling

Usually this type of modelling is based on a service availability calculation by zone of constant headway and by service in order to take into account the impact on one perturbation on one route on the other routes. The cutting between zone permits to have a better service disturbance model than considering only services independently. For an incident on one zone, the impact is modelled on all the line and routes. The RAMS modelling requires the identification of the following:

- **Method and assumptions**
    - **Impact of failures** – identify the categories of failure in order to assess the level of impact in terms of service disruption
    - Method of calculation – the performance indicator “service availability” is based on the number of successful trip. A train that does not fulfill these requirements is considered as an unsuccessful trip or lost trip
    - **Assumptions on operation** – according to the preliminary baseline service plan usually the following data are taken into account as the basis for operation conditions of: rolling stock, traffic forecasts, and train distribution on branches
    - **Assumptions on reserve train** – according to the preliminary baseline service plan and the fleet size it can be arranged the allowance of reserve trains for operation during on-peak hour

- **Assumptions regarding degraded modes** – depending of the degraded modes, different assumptions on regulation mode can be made (a) "negligible" or (b) "delay on line"

- **Failure category analysis**
  - **Impact of "negligible" failure category** – there is no impact on operation
  - **Impact of "delay on line" failure category** – in case of failure of onboard or trackside equipment leading to train stop or delay on the line, the corresponding service disturbance is accounted for the purpose of the theoretical modelling at the terminal station of each zone. Delay on line failure category affects the service availability for each train that arrive at the destination station platform with a delay of more than one headway
  - **Impact of "end of round trip" failure category** – on operation can be modelled per zone and per global effect of "end of round trip"
  - Impact of "return to depot" failure category – on operation can be modelled per zone, per global impact of "return to depot"
  - **Impact of "rescue" failure category** – following a rescue failure category, the rescuing unit train is no longer considered as in operation. Thus, both the rescuing and the rescued trains contribute to lost turns (2 lost trips). The consist of the coupled trains runs to the closer stabling section in order to perturb the traffic at the minimum
  - **Impact of "miss of station" failure category** – in case of failure of trackside equipment or station safety requirements leading to a train cannot stop at a station. In case of onboard equipment leading to miss a station, train is withdrawn and lost trips are counted in "return to depot"

10.0 RAMS documentation

RAMS document	Level System	Level Subsystem	Phase 1 Prelim. Engr.	Phase 1 Prelim. Design	Phase 2 Detailed design	Phase 2 Install T&C
Systems assurance plan	L		X			
Subsystems assurance RAMS plans		L		X		
FRACAS Plan	L	P			X	
Preliminary RAMS apportionment, associated modeling	L	P	X			
Final RAMS apportionment	L	P		X		
Preliminary criticality analysis		L		X		
RAM analysis and prediction studies		L		X	X	
System RAMS report	L				X	
RAMS demonstration plans	L	L			X	
RAMS demonstration test report	L	L				X

Where:
L = Leader, P = Participating