# OCORA

**Open CCS On-board Reference Architecture**

## RAMS – RAM Strategy

Document ID: OCORA-TWS07-050

Version: 1.01

Date: 21.06.2022

# Management Summary

As for vital and safety related systems the safety and, during the last years the (cyber) security, are seen as major challenges, it must not be forgot that on the long run the availybility of the system is key for customer acceptance. As the CCS including its subsystems are quite complex, it is essential to have a clear strategy for reaching a well balanced system, which is not only safe & secure, but also very high available at reasonable component and maintenance cost. Such a strategy mitigates the risk of getting lost in the complex process of working out RAM requirements.

The "OCORA RAM Strategy" sketches the path from the starting point to the goal and the activities required to achieve it. These activites reproduced from the well kown book on “Reliability Engineering – Theory and Practice” [11] involve:

- the marketing
- the development
- the prototyping, and
- the assurance

as mandatory roles with alternating duties as:

- Responsibles (R),
- Cooperation (must), and
- Information (can).

# Revision history

| Version | Change Description | Initial | Date of change |
|---|---|---|---|
| 0.01 | Draft for Release R2. Document ready for review. | EZ | 17.05.2022 |
| 0.02 | Consideration of the review comments | AP | 08.06.2022 |
| 1.00 | Update release for R2 | JB | 09.06.2022 |
| 1.01 | Answer to PV (NS) comments<br>Official release for  R2 | AP | 21.06.2022 |

# Table of Contents

# Table of figures

# Table of Tables

# References

Reader’s note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-010 – Problem Statements

[7] EN 50126-1:2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[8] TS 50701: 2022-01 – Railway applications - Cybersecurity

[9] EN 61703: 2016 – Mathematical Expressions for Reliability, Availability, Maintainability and Maintenance Support Terms (IEC 61703: 2016)

[10] IEC 60050-191 incl. Amendment 1 & 2 – International Electrotechnical Vocabulary (IEV) – Part 191: Dependability and Quality of Service

[11] Alessandro Birolini, “Reliability Engineering – Theory and Practice”, Springer, 8th Edition, 2017.

[12] OCORA-TWS01-030-System-Architecture

[13] Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, SUBSET-091

# 1 Introduction

## 1.1 Purpose of the document

This document – the “OCORA RAM Strategy” - defines the procedure to specify the RAM targets of the OCORA CCS and its subsystems for

- Phase 0 “Prerequisites” of the TS 50701 [8] and
- Phase 1 “Concept” until
- Phase 5 “Architecture and apportionment of system requirements” of the EN 50126-1 [7].

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

## 1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

## 1.3 Context of the document

This document is published as part of an OCORA release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

The Whitepaper on RAM Strategy is connected to other RAMS deliveries, like this document, which are also part of the R2 release. The Figure 1 presents the link between the different deliverables. It must be noticed that the Whitepapers on SRAC/AC Management, on Evolution Management, on Optimized Approval Process and on RAM Strategy are additional documents besides the documents according to the formal CENELEC V cycle Documentation (represented in brown in the figure below) required for the new modular approach.

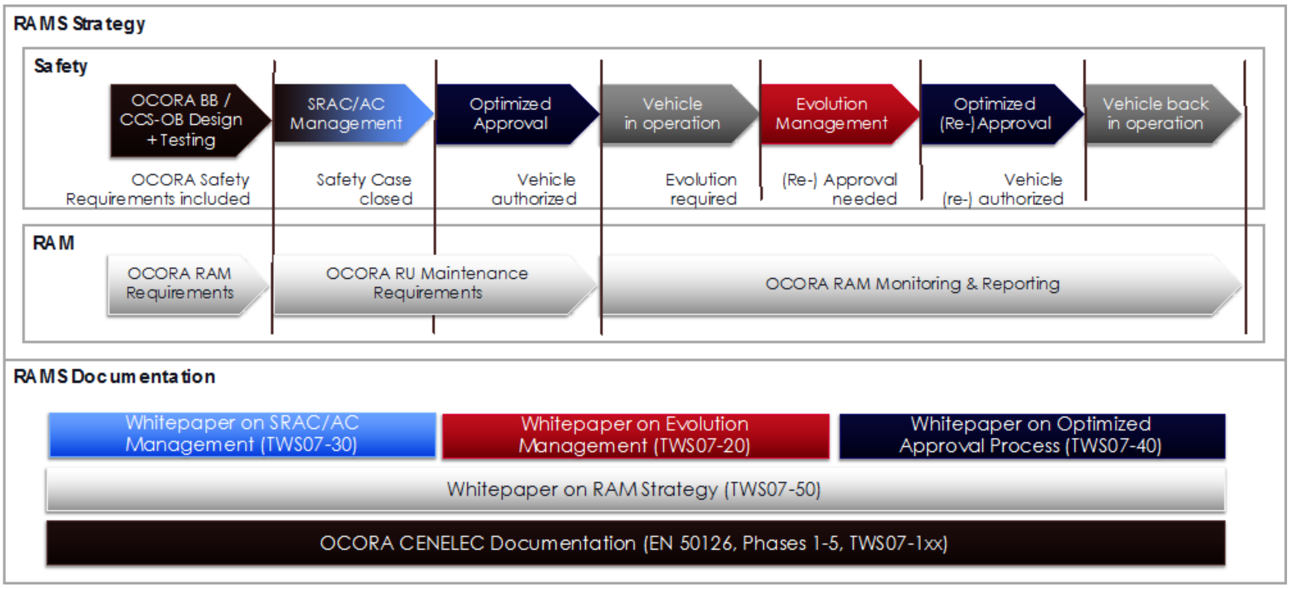
RAMS Strategy
Safety
OCORA BB / CCS-OB Design + Testing
SRAC/AC Management
Optimized Approval
Vehicle in operation
Evolution Management
Optimized (Re-)Approval
Vehicle back in operation
OCORA Safety Requirements included
Safety Case closed
Vehicle authorized
Evolution required
(Re-) Approval needed
Vehicle (re-) authorized
RAM
OCORA RAM Requirements
OCORA RU Maintenance Requirements
OCORA RAM Monitoring & Reporting
RAMS Documentation
Whitepaper on SRAC/AC Management (TWS07-30)
Whitepaper on Evolution Management (TWS07-20)
Whitepaper on Optimized Approval Process (TWS07-40)
Whitepaper on RAM Strategy (TWS07-50)
OCORA CENELEC Documentation (EN 50126, Phases 1-5, TWS07-1xx)

Figure 1: OCORA RAMS Strategy and RAMS Documentation

# 2 Overview of the OCORA RAM Strategy

The purpose of OCORA is to specify the open on-board CCS reference architecture with the goal of enabling the successful integration of all required subsystems/components from different vendors into a:

- reliable,
- safe,
- cybersecure,
- fully functional, and
- approvable

onboard CCS.

This document – the “OCORA RAM Strategy” - defines the procedure to specify the RAM targets of the OCORA CCS and its subsystems. The document aims:

- at ensuring common RAM targets for the CCS as a whole and its subsystems at the system- and its architecture-level.
- at ensuring the RAM targets of the CCS and its subsystems for organizations developing, installing, operating, maintaining, and decommissioning CCS or its subsystems.
- at clarifying the adherence to relevant standards and common regulations.
- at resolving conflicts between RAM and other aspects of the CCS such as safety and (cyber) security (see section 7.3.2.1 in EN 50126-1: 2017 [7]) considering the synchronization points introduced in section 5.1, 5.2, 5.3, 5.5.5, Table 1 and Fig. 6 of TS 50701 [8].

For this purpose, this document presents an outline of the main RAM activities that will be subsequently carried out within OCORA:

- compiling common RAM targets of the existing CCS as a whole and its subsystems as a starting point,
- specifying the RAM targets of the OCORA CCS and its subsystems, which are the project goals.

The scope of this “OCORA RAM Strategy” is restricted to:

- Phase 0 “Prerequisites” of TS 50701 [8] and
- Phase 1 “Concept” until
- Phase5 “Architecture and apportionment of system requirements” of EN 50126-1 [7].

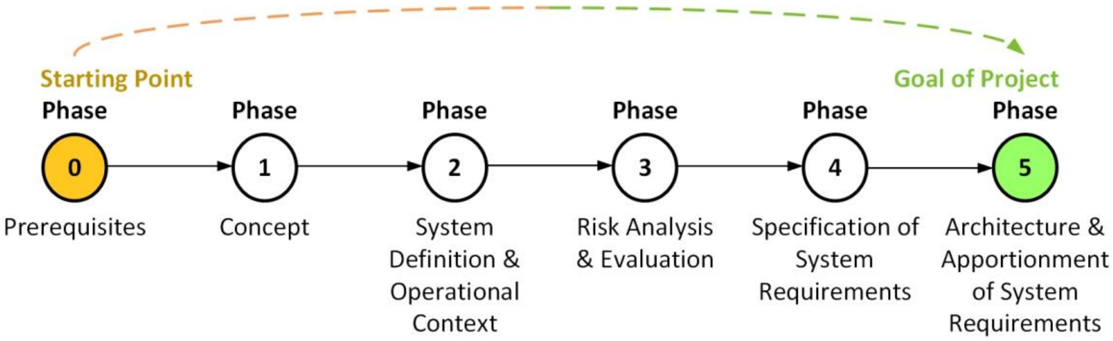
Starting Point
Goal of Project
Phase
0
Prerequisites
Phase
1
Concept
Phase
2
System Definition & Operational Context
Phase
3
Risk Analysis & Evaluation
Phase
4
Specification of System Requirements
Phase
5
Architecture & Apportionment of System Requirements

Figure 2: Scope of the RAM strategy covering Phase 0 from the TS 50701 [8] and Phase 1 until Phase 5 from EN 50126-1 [7]

# 3 Starting Point of the RAM Strategy

The starting point of the RAM strategy is

- the definition of the System under Consideration (SuC) provided in [12],
- its overall Reliability Targets (RTs) of the existing CCSs,
- the RTs of the subsystems of existing CCSs,
- the RTs of the communication links (incl. physical interfaces) among the sub-systems of existing CCSs,
- the RTs of the communication link(s) of existing CCSs to the outside world,
- the RT of peripheral subsystems of existing CCSs',
- the mission profile of each item under consideration (refer also to Chapter 10 of subset-091 [13]) and
- the testability of the system.

The Reliability $R$ is a characteristic of an item, expressed by the probability that it will perform its required function under given conditions for a stated time interval. The concept of reliability applies to nonrepairable as well as repairable items. To make sense, a numerical statement of reliability (e.g. $R = 0.9$) must go by the definition of:

- the **required function**. It specifies the item's task, i.e. for given inputs, the item's outputs have to be constrained within specified tolerance bands. The definition of the required function is the starting point for any reliability analysis, as it defines failure.
- the **operating conditions**. Operating conditions have an important influence on reliability, and must therefore be specified with care. Note that the failure rate of semiconductor devices will double for operating temperature increase of 10°C to 20°C.
- the **mission profile**. The required function and/or operating conditions can be time dependent. In these cases, a mission profile has to be defined and all reliability figures will be related to it.
- whether the item can be considered new when the mission starts.

The mission duration is considered as a parameter $t$. The reliability function is then defined by $R(t)$. $R(t)$ is the probability that no failure at item level will occur in the interval $(0, t]$.

The failure rate $\lambda(t)$ (see [9], [11]) is given by

$$\lambda(t) = \frac{-\frac{d}{dt}R(t)}{R(t)}.$$

This definition of the failure rate $\lambda(t)$ applies in particular to non-repairable items. However, $\lambda(t)$ can also be defined for repairable items which are as-good-as-new after repair.

In many practical applications, $\lambda(t) = \lambda$ can be assumed. In this case:

$$R(t) = e^{-\lambda t}.$$

The Mean Time To Failure $MTTF$ is given by

$$MTTF = \int_{0}^{\infty} R(t)\, dt.$$

Considering that the item is as-good-as-new after each repair, the Mean Time Between Failures $MTBF$ is

$$MTBF = \frac{1}{\lambda}.$$

Note that $MTBF$ stands for Mean operating[1] Time Between Failures.

The starting point of this RAM strategy states only RT as listed in Table 6-1 because the Availability and Maintainability cannot be defined in general terms independently from the repair and maintenance processes of the railway operators and it is assumed that these processes differ among the railway operators.

Hence, this RAM strategy considers as starting point

[1] This refers to the operational time of the CCS system; it does not necessarily correspond to the time when the train is "in operation".

- **the probability of a failure $F_D$ per unit distance the train travelled for the CCS or its subsystems.**
- **the failure rate $\lambda$, i.e. the probability of a failure per unit time for a communication link.**

# 4 Goals of the RAM Strategy

The goal of the OCORA RAM strategy is to specify all RAM Targets at

- the level of the overall CCS system specified in [12],
- the subsystems of the CCS architecture specified in [12],
- the communication links between the components of the CCS architecture, and
- the communication links of the CCS system to the outside world.

The corresponding Reliability, Availability, and Maintainability parameters are listed in Table 6-1, Table 6-2, and Table 6-3, respectively. Possible Logistics Support Parameters are listed in Table 6-4.

In general, any time-based parameter like $MTBF$ can be converted/derived from the respective operated distance or operation cycles as well.

Definition and detailed guidance on mathematical treatment of RAM terms is given in EN 61703 [9].

The formulas for the calculation or conversions of the RAM parameters into one another are provided in Annex B (chapter 6). Note that these formulas assume a constant failure rate $\lambda$.

For additional mathematical expressions for Reliability, Availability, Maintainability and Maintenance Support Term, the reader is referred to

- Annex B of EN 50126-1 [7],
- EN 61703 [9], and
- IEC 60050-191 [10].

Using these formulas, the railway operator can calculate the full set of RAM parameters for different CCS or CCS subsystem suppliers considering his repair and maintenance processes and the supplier's predicted reliability targets.

Note that the investigation of the failure rate $\lambda$ of a complex equipment or system leads to the calculation of the *predicted reliability*, i.e., that reliability which can be calculated from the structure of the item and the reliability of its elements. Such a prediction is necessary for an early detection of reliability weaknesses and for comparative studies.

Because of different kinds of uncertainties, the predicted reliability can often be only given with a limited accuracy. To these uncertainties belong

- simplifications in the mathematical modelling (independent elements, complete and sudden failures, no flaws during design and manufacturing, n0 damages),
- insufficient consideration of faults caused by internal or external interference (switching, transients, EMC, etc.),
- inaccuracies in the data use for the calculation of the component failure rates.
- Insufficient consideration of human errors in operation or maintenance
- Insufficient consideration of future changes in operational profile

On the other hand, the true reliability of an item can only be determined by reliability tests, performed often at the prototype's qualification tests, i.e., late in the design and development phase. Practical applications also shown that with an experienced reliability engineer, the predicted failure rate at equipment or system level often agree reasonably well (within a factor of two) with field data. Moreover, relative values obtained by comparative studies generally have a much greater accuracy than absolute values. All these reasons support the effort for a *reliability prediction* during the design of equipment and systems with specified reliability targets.

Besides theoretical considerations, practical aspects have to be considered when designing reliable equipment and systems, for instance with respect to operating conditions, human factors and to the mutual influenced between elements (input / output, load sharing, effects of failures, transients, etc.).

Required function and environmental conditions are often time dependent, leading to a mission profile (operational profile for software). A

- representative mission profile and
- a representative set of operating conditions

shall be stated with the predicted reliability targets in the system specifications for the CCS as a whole and each of its architectural constituents, i.e. subsystems.

# 5 RAM Activities

## 5.1 Overview

According to the EN 50126-1 [7],

1. the Reliability activities shall include:
   - reliability analysis and prediction,
   - reliability planning,
   - reliability testing, and
   - reliability data acquisition and assessment.
2. the Availability activities shall include:
   - availability analysis,
   - sensitivity analysis, and
   - availability data acquisition and assessment.
3. the Maintainability activities shall include:
   - maintainability analysis and prediction,
   - maintainability planning, and
   - logistic support evaluation.

These activities are implemented in the order shown in Table 5-1 of section 5.4. Phases 0 and 1 are currently being implemented and are therefore described in more detail in sections 5.2 and 5.3.

## 5.2 Phase 0 (Prerequisites): Customer and Market Requirements

The customer and market requirements include

- the evaluation of delivered equipment and systems and
- the determination of market and customer demands and needs.

For this purpose, a common OCORA functional/physical Work Breakdown Structure (WBS) of existing CCSs shall be defined. This dictionary of OCORA Building Blocks will be used throughout all further RAM analysis as common reference. This allows the assignment of electronic boards of existing CCS from different manufacturers with the same functionalities to one common OCORA LRU. This OCORA WBS will be used extensively during the subsequent “Preliminary RAM Analysis”, i.e. the collection of RAM parameters from different Enterprise Resource Planning (ERP) data bases (usually SAP based) from different European railway undertakings.

## 5.3 Phase 1 (Concept): Preliminary RAM Analysis

In defining quantitative quality and reliability requirements of the OCORA CCS and its subsystems, attention has to be paid to the actual possibility to realize them, as well as to demonstrate them at a final or acceptance test. These requirements are derived from customer or market needs, taking care of limitations given by technical, cost, and ecological aspects.

For this purpose, the specification of the OCORA CCS RAM parameters shall be based on the proven performance figures of existing CCS. The collection of RAM parameters shall be based on:

- “work orders” containing reports (i.a. of the train drivers) about the problems from the operative point of view.
- “repair reports” detailing how the problem has been solved and what had to be replaced, if any. Usually, such repair reports are only available for items outside the warranty period.
- “operational failures” containing information on the operational impact of failures and the possibilities and effectives of failure resolution on track

It is assumed that every Railway Undertaking (RU) maintains these two types of reports in its ERP system and their content is easier to compare among different RUs and different projects than, e.g. “defect reports”.

The collection of RAM data of existing CCS is restricted to reliability data. This is due to the fact, that operational availability and maintainability data heavily depends on many logistic and organizational conditions of the RUs. Additionally, these logistic and organizational conditions differ significantly among different RUs.

The collection of reliability data of existing CCS is based on data obtained from the RUs of the OCORA members, i.e.

- the “Deutsche Bahn AG” (DB),
- the «Nederlandse Spoorwegen N.V.» (NS),
- the «Société Nationale des Chemins de fer Français” (SNCF), and
- the «Schweizerischen Bundesbahnen (SBB).

Possible reliability parameters to be collected are listed in Table 6-1 of Annex A (chapter 6). The formulas listed in Table 7-1 of Annex B (chapter 7) allow the conversion of one set of parameters into another one on common bases.

## 5.4 Basic Tasks for Quality and Reliability Assurance (till phase 5)

CCS and CCS subsystems are considered as complex items. For this reason, quality and reliability are best achieved with a quality and reliability (RAM) assurance program with clearly defined tasks and activities assigned to the responsible roles. The Table 5-1 contains a preliminary example of the quality and reliability assurance program for the phases 0 of TS 50701 [8], and phase 1 until the 5 of EN 50126-1 [7].

Table 5-1: Example of basic tasks for quality and reliability assurance of complex equipment and systems (from [11])

| **Phase** | **Activities**<br><br>**R** Responsible<br>**C** Cooperation (must cooperate)<br>**I** Information (can cooperate) | | **Marketing (M)** | **Development (D)** | **Production (P)** | **Assurance (Q&R)** |
|---|---|---|---|---|---|---|
| **0** | **Customer and market requirements** | | | | | |
| | 1 | Evaluation of delivered equipment and systems | R | I | I | C |
| | 2 | Determination of market and customer demands and needs | R | I | I | C |
| | 3 | Customer support | R | --- | --- | C |
| **1** | **Preliminary RAM analysis** | | | | | |
| | 1 | Definition of tentative quantitative targets for quality & reliability | C | C | C | R |
| | 2 | Rough analysis and identification of potential problems | I | C | --- | R |
| | 3 | Comparative investigations | I | C | --- | R |
| **2** | **Reliability aspects in specifications, quotations, contracts, etc.** | | | | | |
| | 1 | Definition of the required function(s) | I | R | --- | C |
| | 2 | Determination of (external) environmental conditions | C | R | --- | C |
| | 3 | Definition of realistic quantitative targets for quality & reliability (refer also to the items explained in section 5.3). | C | C | C | R |
| | 4 | Specification of test and acceptance criteria | C | C | C | R |
| | 5 | Identification of the possibility to obtain field data | R | --- | --- | C |
| | 6 | Cost estimate for quality & reliability assurance activities | C | C | C | R |
| **3** | **Quality and Reliability assurance program** | | | | | |
| | 1 | Preparation | C | C | C | R |
| | 2 | Realisation<br>• Design and evaluation<br>• Production | <br>I<br>I | <br>R<br>I | <br>I<br>R | <br>C<br>C |
| **4** | **Reliability and maintainability analysis** | | | | | |

| Phase | Activities<br>**R** Responsible<br>**C** Cooperation (must cooperate)<br>**I** Information (can cooperate) | | Marketing (M) | Development (D) | Production (P) | Assurance (Q&R) |
|---|---|---|---|---|---|---|
| | 1 | Specification of the required function of each subsystem | --- | R | --- | C |
| | 2 | Determination of environmental, functional, and time-dependent stresses (detailed operating conditions) | --- | R | --- | C |
| | 3 | Assessment of derating factors | --- | C | --- | R |
| | 4 | Reliability and maintainability allocation | --- | C | --- | R |
| | 5 | Preparation of reliability block diagram<br>• Assembly level<br>• System level | <br>---<br>--- | <br>R<br>C | <br>---<br>--- | <br>C<br>R |
| | 6 | Identification and analysis of reliability weaknesses (FMEA/FMECA, FTA, worst-case, drift, stress-strength-analysis, etc.)<br>• Assembly level<br>• System level | <br>---<br>--- | <br>R<br>C | <br>---<br>--- | <br>C<br>R |
| | 7 | Carrying out comparative studier<br>• Assembly level<br>• System level | <br>---<br>--- | <br>R<br>C | <br>---<br>--- | <br>C<br>R |
| | 8 | Reliability improvement through redundancy<br>• Assembly level<br>• System level | <br>---<br>--- | <br>R<br>C | <br>---<br>--- | <br>C<br>R |
| | 9 | Identification of components with limited lifetime | I | R | --- | C |
| | 10 | Elaboration of the maintenance concept | I | R | I | C |
| | 11 | Elaboration of a test and screening strategy | C | C | C | R |
| | 12 | Analysis of maintainability | --- | R | --- | C |
| | 13 | Elaboration of mathematical models | --- | C | --- | R |
| | 14 | Calculation of the predicted reliability and maintainability<br>• Assembly level<br>• System level | <br>I<br>I | <br>R<br>C | <br>---<br>--- | <br>C<br>R |
| | 15 | Reliability and availability calculation at system level | I | I | --- | R |
| **5** | **Human factor analysis** | | | | | |
| | 1 | Analysis of safety (avoidance of liability problems)<br>• Accident prevention<br>• Technical Safety<br>– Identification and analysis of critical failures and of risk situations (FMEA/FMECA, FTA, etc.)<br>○ Assembly level<br>○ System level<br>– Theoretical investigations | <br>C<br><br><br>---<br>I<br>--- | <br>R<br><br><br>R<br>C<br>C | <br>C<br><br><br>---<br>---<br>--- | <br>C<br><br><br>C<br>R<br>R |
| | 2 | Analysis of human and ergonomic factors | C | R | C | C |

# 6 Annex A - RAM Parameters

The reliability, availability, maintainability and logistics support parameters are listed in Table 6-1, Table 6-2, Table 6-3, and Table 6-4, respectively. They are partly taken from Annex B of EN 50126-1 [7].

Table 6-1: Reliability Parameters

| Quantity | Symbol | Unit |
|---|---|---|
| Failure rate | $\lambda$ | 1/time, 1/distance, 1/cycle |
| Mean Up Time | $MU\,T$ | time (distance, cycle) |
| Mean operating[a] Time To Failure<br>(for nonrepairable items) | $MTTF$ | time (distance, cycle) |
| Mean operating[a] Time Between Failure<br>(for repairable items) | $MTBF$ | time (distance, cycle) |
| Failure Probability | $F$ | dimensionless |
| Reliability (success probability) | $R$ | dimensionless |
| [a] According to EN 61703 [9] and IEC 60050-191 [10]. | | |

Table 6-2: Availability Parameters

| Quantity | Symbol | Unit |
|---|---|---|
| Availability<br>• inherent<br>• operational | $A$<br>$A_i$<br>$A_o$ | dimensionless<br>dimensionless<br>dimensionless |
| Unavailability<br>• inherent<br>• operational | $U$<br>$U_i$<br>$U_o$ | dimensionless<br>dimensionless<br>dimensionless |
| Failure Frequency | $w$ | 1/time, 1/distance, 1/cycle |
| Repair Rate | $\mu$ | 1/time, 1/distance, 1/cycle |
| Inspection Interval | $\tau$ | time |
| Mean Time Between Failures | $MTBF$ | time |
| Fleet Availability | $FA$ | dimensionless |
| Schedule Adherence | $SA$ | dimensionless |

Table 6-3: Maintainability Parameters

| Quantity | Symbol | Unit |
|---|---|---|
| Mean Down Time | $MDT$ | time (distance, cycle) |
| Mean operating[a] Time Between Maintenance | $MTBM$ | time (distance, cycle) |
| Mean Time Between Maintenance<br>(corrective or preventive) | $MTBM(c)$<br>$MTBM(p)$ | time (distance, cycles) |
| Mean Time To Maintain | $MTTM$ | time |
| Mean Time To Maintain<br>(corrective or preventive) | $MTTM(c)$<br>$MTTM(p)$ | time |

| Quantity | Symbol | Unit |
|---|---|---|
| Mean Time To Restore | $MTTR$ | time |
| Mean Repair Time | $MRT$ | time |
| Fault Coverage | $FC$ | dimensionless |
| Repair Coverage | $RC$ | dimensionless |
| [a] According to EN 61703 [9] and IEC 60050-191 [10]. | | |

Table 6-4: Logistic Support Parameters

| Quantity | Symbol | Unit |
|---|---|---|
| Operation and Maintenance Cost | $O\&MC$ | money |
| Maintenance Cost | $MC$ | money |
| Maintenance Man Hours | $MMH$ | time (hours) |
| Mean Logistic Delay | $MLD$ | time |
| Mean Administrative Delay | $MAD$ | time |
| Fault Correction Time | $FCT$ | time |
| Turn Around Time | $TAT$ | time |
| Maintenance support performance | $MAT$ | dimensionless |
| Employees for Replacement | $EFR$ | number |
| Probability that Spare Parts are available (in Stock) when needed | $SPS$ | dimensionless |

# 7 Annex B – Calculation of RAM Parameters

## 7.1 Formulas for the Calculation of various RAM Parameters

Table 7-1 contains the formulas for the calculation of various RAM parameters some of which are based on the “dormant” failure model. The “dormant” failure model is described in section 7.2.

Table 7-1: Calculation of RAM parameters

| **Quantity** | **Symbol** | **Formulas** |
|---|---|---|
| *Unavailability* | $U$ | $U = 1 - A = 1 - \frac{w}{\lambda} = \frac{\lambda}{\lambda + \mu} = \frac{w}{\mu} = \frac{MDT}{MTTF + MDT}$<br>and as a function of $\tau$:<br>$U = \frac{\lambda\,\tau - \left(1 - e^{-\lambda\tau}\right) + \lambda \cdot MTTR \cdot \left(1 - e^{-\lambda\tau}\right)}{\lambda\,\tau + \lambda \cdot MTTR \cdot (1 - e^{-\lambda\tau})}$<br>for the "Dormant" failure model<br>$U \approx \lambda\left(MTTR + {}^{1}/_{2}\right) = \frac{1}{2}\left(1 - \sqrt[2]{1 - 4\,w\left(MTTR + {}^{1}/_{2}\right)}\right)$<br>for the "Dormant" failure model (approximation) |
| *Availability* | $A$ | $A = 1 - U = \frac{w}{\lambda} = \frac{\mu}{\lambda + \mu} = \frac{\mu - w}{\mu} = \frac{MTTF}{MTTF + MDT}$ |
| *Failure frequency* | $w$ | $w = \lambda\,A = \lambda\,(1 - U) = \frac{\lambda\,\mu}{\lambda + \mu}$<br>and as a function of $\tau$:<br>$w = \frac{2\,U\,(1 - U)}{\tau + 2\,MTTR}$<br>for the "Dormant" failure model |
| *Failure rate* | $FR, \lambda$ | $\lambda = \frac{1}{MTTF} = \frac{w}{A} = \frac{w}{1 - U}$<br>and as a function of $\tau$:<br>$\lambda = \frac{2\,U}{\tau + 2\,MTTR}$<br>for the "Dormant" failure model |
| *Repair rate* | $\mu$ | $\mu = \frac{1}{MTTR} = \frac{w}{U}$ |
| *Inspection interval* | $\tau$ | $\tau = 2\,\frac{U - \lambda \cdot MTTR}{\lambda}$<br>for the "Dormant" failure model |
| *Mean Repair Time* | $MRT$ | MDT – failure disclosure time |
| *Mean Time To Failure* | $MTTF$ | $MTTF = \frac{1}{\lambda} = \frac{A}{w} = \frac{1 - U}{w}$ |

| Quantity | Symbol | Formulas |
|---|---|---|
| *Mean Time To Restore* | $MTTR$ | $MTTR = \frac{1}{\mu}$<br>and as a function of $\tau$:<br>$MTTR = \frac{U}{w}$ for $\tau \to 0$ or models without $\tau$ $(MTTR = MRT)$<br>$MTTR = \frac{2\,U - \lambda\,\tau}{2\,\lambda}$<br>for the "Dormant" failure model |
| *Mean Time Between Failures* | $MTBF$ | $MTBF = MTTF + MDT, \qquad MTBF = \frac{1}{w} = \frac{1}{\lambda\,A} = \frac{1}{\lambda\,(1-U)}$ |
| *Mean Down Time* | $MDT$ | $MDT = \frac{U}{w}$<br>general and moreover:<br>$MDT \to MRT\ for\ \tau \to 0$ or modls without $\tau$<br>$MDT = \frac{\tau + 2 \cdot MRT}{2\,(1-U)}$<br>for the "Dormant" failure model |

## 7.2 Dormant Failure Model

Dormant failure modes have no direct impact on the system because a redundant system or element automatically steps in, or if the failure is only problematic during certain mission or system states, such as latent failures that have a deterioration mechanism such as a growing metal crack that does not yet reach a critical length. Dormant failure modes are failures that are not immediately revealed, i.e. latent or hidden.

The “dormant” failure model accounts for periodic inspections that reveal dormant failures during maintenance or inspection.

For the dormant failure model, the subsequent formulas apply.

The mean value of the unavailability $Q_{mean}$ is given by

$$Q_{mean} = \frac{\lambda\,\tau - \left(1 - e^{-\lambda\tau}\right) + \lambda \cdot MTTR \cdot \left(1 - e^{-\lambda\tau}\right)}{\lambda\,\tau + \lambda \cdot MTTR \cdot (1 - e^{-\lambda\tau})},$$

where

- $\lambda$ denotes the constant failure rate,
- $MTTR$ is the Mean Time To Repair, and
- $\tau$ is the inspection interval.

If $\lambda \cdot \tau \ll 1$ and $\lambda \cdot MTTR \ll 1$,

$$Q_{mean} \cong \frac{\lambda\,\tau}{2} + \lambda \cdot MTTR\,.$$

The dormant failure model also allows the modelling of detected failures. For this purpose, $\tau$ must approach zero $(\tau \to 0)$. Hence,

$$\lim_{\tau \to 0} Q_{mean} \cong \frac{\lambda \cdot MTTR}{1 + \lambda \cdot MTTR}\,.$$