

SYSTEM ASSURANCE BY IN-SERVICE RELIABILITY EVALUATION

S.W. Mealing*, W. Hinsley †

*Transsol Ltd: Email: smealing@transsol.net † Transsol Ltd: Email: whinsley@transsol.net

Keywords: Reliability, Dependability, Safety, Maintainability, Availability.

1 Introduction

Modern day railway systems and equipment are often required to be assessed against numeric targets, be they contractual or dictated by defined safety requirements, prior to acceptance into service of the system and/or equipment [1].

These numeric targets can take the form of availability or reliability figures, expressed in units of time, or as dimensionless probabilities of failure on demand.

As well as theoretical predictions that these targets will be met, a period of reliability monitoring is necessary to confirm that the theoretical predictions and/or design/safety requirements have been realised by the in-service operation of the equipment.

The main objective of reliability demonstration testing is to obtain a meaningful measure of the monitored systems/equipment in-service availability and reliability. However such testing can have benefits beyond the area of system assurance and provide the necessary data to create an effective programme of reliability centred maintenance and reliability improvement.

It is often the case that this data is seemingly obtained via methodical means when in fact it is not. Whenever there are requirements for personnel involved in a fault recording system to make subjective judgments about the nature of faults, or to describe what they have observed, they bring with them an element of uncertainty into the data recorded. This has the potential to undermine the subsequent assessments by the data lacking the consistency necessary for accurate analysis of reliability performance.

The solution to the problem is to provide a total fault recording and corrective action system (FRACAS) that is based entirely on pre-defined base information. Coupled with a relational database, designed specifically to mirror the format of the initial fault recording to store and automatically analyse the data, a rigorous and consistent means of measuring in-service reliability performance can be achieved.

The paper will describe the means by which rigour and consistency of collated reliability data is ensured and how the

data can be recorded, stored and analysed in an efficient manner.

2 Reliability Demonstration Testing - Overview

Numeric targets defined for modern systems, particularly safety critical systems, require availabilities that are measured in terms of one failure per several million hours of operation.

With limited populations of equipment in-service and with limited time frames for reliability demonstration testing (RDT) it is essential to define pass/fail criteria. The means to establish pass/fail criteria (i.e. the tolerable numbers of failures) are well established and reported in various European and International standards [2 and 3].

To allow assessment of the pass/fail criteria it is important to know precisely what information needs to be recorded, have a system to accurately record, store and analyse the information and, not least, to make this easy to understand and to use.

The FRACAS is used to collect information on all events that might cause 'down-time' of the system(s) under test; these events fall into one of three categories:

- Faults.
- Corrective actions.
- Maintenance activities.

The key requirements are to be able to record all of the relevant information from systems under test in a consistent and rigorous manner, to allow analysis of the data and to provide clear presentation of the results.

All of the relevant information about a system or item of equipment under test must be precisely defined. This information can then be uniquely coded for use with an appropriately designed FRACAS. When this approach is combined with the appropriate organisation and training the RDT exercise can provide the rigour and consistency demanded of it.

3 RDT Organisation and Training

Implementing a RDT programme involves a number of interested parties. Typically these include:

- Owner/operator of the system.
- Supplier/manufacturer.
- Installer/maintainer.

- Third party implementing the RDT FRACAS (if not part of owner or supplier organisation).

An organisation structure identifying the parties that have an input to the RDT is shown in figure 1.

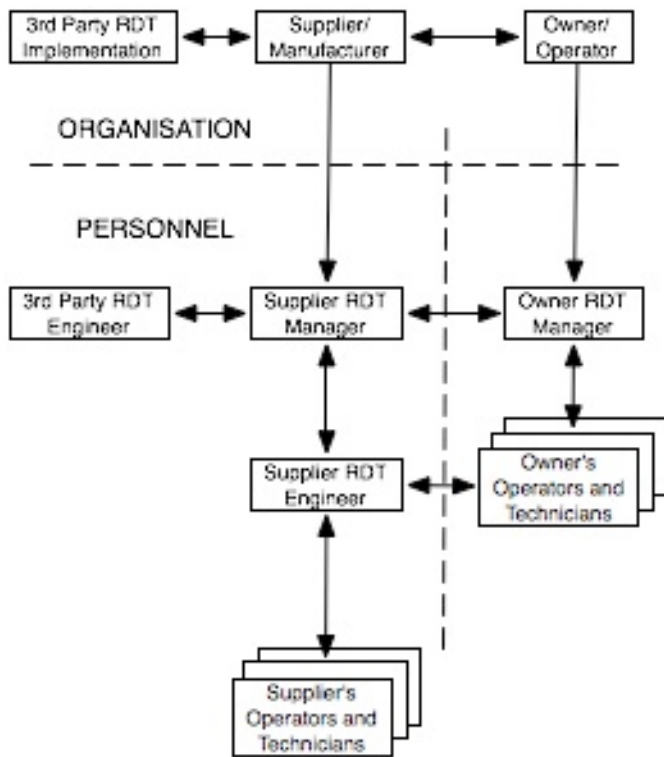


Figure 1 - Organisation

At an organisational level there is a need to establish agreements in respect of the equipment to be included in the RDT exercise, the precise definition of system failure or unavailability, the relevance of identified failure modes and pass/fail criteria.

At the personnel level the main activities carried out are as follows:

- Identifying fault conditions/maloperation.
- Investigating faults and recording the details.
- Performing corrective actions and recording details.
- Performing maintenance activities and recording details.
- Verifying recorded data.
- Entering data into the database.
- Analysis and reporting.

It is important to establish who is responsible for what in terms of the personnel within each organisation.

Adequate training must also be provided for all staff involved in the RDT exercise. The training must be structured so as to be relevant to each individual's role in the process. The responsibility for providing training lies with the RDT Managers.

4 General Methodology

The reliability of a system is defined as the probability that the system will not fail in a given period of time. To estimate the reliability of a system it is necessary to record:

- The total number of relevant faults;
- The total relevant operating time.

The availability of a system is defined as the probability that at any time the system is operating normally. To estimate the availability of a system it is necessary to record:

- The total relevant operating time;
- The total relevant system down-time.

Equipment failures will be classified as being 'always relevant', 'sometimes relevant' or 'never relevant' to the testing.

Failures that are 'always relevant' are those failure modes that affect vital system functions and will, by themselves, result in loss of safety or other vital functionality. These faults affect the reliability and availability of the system.

Failures that are 'sometimes relevant' are those failure modes affecting vital system function only under certain circumstances, e.g. if occurring coincidentally with another un-related failure. If a 'sometimes relevant' failure occurs coincidentally with another fault condition and results in loss of vital system function then under these conditions the fault is classed as a relevant failure.

Failures that are 'never relevant' cannot affect vital system functions.

The relevant operating time is the total time that the system is under test and operating normally. The relevant operating time excludes any system down time due to faults (whether relevant or non-relevant), corrective actions and maintenance. To calculate the total relevant operating time therefore requires that all activities that might affect the operation of the system be recorded, i.e. it is necessary to record all maintenance activities as well as faults and corrective actions.

The relevant down time is the total time that a vital function of the system is not available; i.e. the system is failed (down). Down time due to relevant failure, preventative maintenance or corrective maintenance will all be classified as relevant. Any causes of non-relevant down time must be defined; non-relevant down time is excluded from the total relevant operating time and is not added to the total relevant downtime. An example of non-relevant downtime is that resulting from an interface failure (e.g. loss of external power supplies).

5 Fault Recording and Corrective Action System

The FRACAS comprises the following main elements:

- A form based data collation system.

- Code catalogues.
- RDT Test Plans.
- A computerised database for effective storage and analysis of the data.
- Guidelines controlling the data collation, analysis and reporting processes.

Data Collation Forms

All of the information collated as part of the RDT is recorded on specific forms. There are three different forms used for recording:

- Faults.
- Corrective actions.
- Maintenance activities.

Each form is designed to be as simple as possible whilst still allowing all of the necessary information to be recorded. The main feature of the RDT described in this paper is that all of the information recorded on the forms has been assessed and precisely defined prior to commencement of the RDT. In turn this information has been uniquely coded and the codes listed in a code catalogue. In this way any and all information that needs to be entered onto the data collation forms is contained in the code catalogues, there is no requirement for subjective judgements to be made by personnel involved in the fault recording activities.

This is the key to the consistency and quality of the recorded data and enables a meaningful measure of a system's in-service reliability/availability to be obtained.

The fault data collation form is completed following any failure or malfunction of the equipment subject to RDT whether or not it is considered to be relevant. One form is raised for each identified fault and each form contains the following information:

- Unique fault reference.
- Details of how the fault was identified.
- Details of faulty equipment and failure modes
- Secondary failures
- Operating & environmental conditions at the time of the fault

The corrective action form is completed following any maintenance work undertaken to rectify an identified fault. One form is raised for each corrective action undertaken and each form contains the following information:

- Unique corrective action reference linked to corresponding fault report.
- Confirmation of the original fault.
- Specific equipment affected by corrective action.
- Details of any equipment replaced.

- Details of any adjustments made.
- Success/failure of corrective action.

The maintenance form is required for capturing any maintenance activity, scheduled or un-scheduled, that is not performed to rectify an identified fault. There is one form for each maintenance activity undertaken and each form contains the following information:

- Unique maintenance action reference.
- Specific equipment affected by the maintenance.
- Details of any equipment replaced.
- Details of any adjustments made.

The data collation forms are designed to make it clear who is required to complete each section and have a logical structure to make them easy to understand and use.

Code Catalogues

The system of coding ensures, as far as is possible, that standard data is entered into the data collation forms and also removes the need for subjective judgments from the operators and technicians.

The coding system includes five categories of code:

- Systems: Each system under test has a unique code.
- Locations: Each location in which equipment is installed is given a unique code; the coding can reflect varying degrees of precision for where specific equipment is located.
- Equipment: Each type of line replaceable unit included in the reliability testing has a unique code.
- Installations: Every instance of equipment that comprises the system under test has a unique code.
- Failure modes: The failure modes of systems and equipment are predefined and each is given a unique code.

A code catalogue is produced listing the systems, locations and installations included in the testing; failure modes of the equipment and systems under test are also included in the code catalogue. For each entry the unique combination of codes required to be entered in the forms are listed. The code catalogue is arranged logically so that locating the codes to describe a particular piece of equipment and its modes of failure is straightforward.

RDT Test Plans

The purpose of the RDT test plan is to present all of the system specific information in a way that allows this information to be reviewed and approved prior to the start of the testing and in a format that can be directly imported into the FRACAS database. Obtaining this agreement at the start of the testing ensures that the results will be accepted by all parties. The RDT test plans are therefore very important documents.

The RDT test plans contain the following information:

- **Equipment definition:** The equipment that constitutes the system and is included in the testing is defined down to line replaceable units.
- **System function:** The functionality of the system is identified and what reduction in function is considered to constitute failure of the system or system unavailability is defined.
- **Relevant failures:** All failure conditions of the system that are considered relevant to the reliability/availability are defined. Any failure conditions that causes the system to be unavailable but that are not relevant are also identified.
- **Failure modes:** Detailed failure modes are defined for each type of LRU. For each failure mode its relevance, or otherwise, is defined and whether any redundancy is affected.
- **Performance targets:** The performance targets for reliability and availability of the system are identified along with the predicted performance.
- **Operations & Maintenance:** The operation & maintenance procedures relevant to the system are identified. Routine maintenance activities are identified and classified as relevant or non-relevant to the reliability or availability tests
- **Monitoring Procedure:** Any special procedures for monitoring the condition of the systems/equipment under test are identified.
- **Relevant Test Time:** The basis for measuring relevant test time is defined.

Failure Modes

Two sets of failure modes are defined. The first set describes how faults and failures affect the overall functionality of the system; these are intended to allow faults to be recorded initially without knowledge of the causes and specific equipment affected. The second set of failure modes describe the faults and failures that affect specific items of equipment; these are intended for use by technicians in accurately recording the causes and consequences of system faults.

For the top-level system failure modes this consists of:

- The system
- Title and description of the defined system failure mode.
- The consequence.
- Unique code number.

For the specific equipment failure modes this consists of:

- The equipment type.
- Title and description of the defined failure mode.
- The consequence.

- Its relevance.
- The effect on redundancy.
- Unique code number.

Note that relevance is not defined for system failure modes as the relevance depends on the precise cause of the failure.

The failure modes are described in tabular form to enable direct import into the database.

FRACAS Database

A database facilitates the management and analysis of the data recorded on the forms. All data recorded on the forms is entered into the database.

The database is a management system used to store and analyse the test data, calculate system performance and present the results in a coherent fashion. It enables a wide range of incoming incident reports (data) to be collected, quantified and controlled such as test and field data and repair and maintenance data.

The database is populated with the reference information contained in the RDT test plans and contains the information that allows:

- Production of the code catalogues that will be used to complete the forms
- Correct analysis of the effects of faults, corrective actions and maintenance activity
- Automatic calculation of the reliability/availability demonstrated by each system under test
- Automatic calculation of scheduled and unscheduled maintenance time

The database makes recording & analysis of the data very straightforward and can also be used for monitoring of system performance and reporting results. This is supported by the following features:

- Secure, reliable and auditable record of reliability testing.
- Real time analysis of test data with summary views showing the performance targets against achieved performance.
- Summary of the test data for each system.
- Automatic generation of reports.

Specific information that is available for each system/equipment includes:

- Accumulated relevant test time.
- Relevant and non-relevant down time.
- Number of relevant failures.
- MTBF achieved.
- Availability achieved.

- Scheduled and unscheduled maintenance time.

Guidelines

A detailed set of guidelines are produced for all aspects of the RDT. Training is carried out specifically tailored to the roles of the personnel involved in the RDT personnel. The training and Guidelines cover the following aspects:

- Roles and responsibilities: who does what within each organisation.
- Processes for recording faults, corrective actions and maintenance activities.
- Specific tasks such as:

- **Raising new forms.**

Obtaining/constructing the unique report numbers from a fault report register. Using the code catalogues for system, equipment, location, installation, failure mode, corrective actions and maintenance data and entering this coded data onto the forms.

- **Verifying the data on the forms.**

Using the power of the FRACAS database's search facilities to validate the coded data entered into it.

- **Checking for and dealing with errors on the forms.**

Procedural role, which is part of the RDT Managers' responsibilities.

- **Handling unlisted failure modes.**

Fields are available in the data collation forms (and FRACAS database) for failure modes not listed in the code catalogues. There is a means defined in the guidelines for adding new reference data into the FRACAS system in a controlled and auditable manner.

- **Entering data from the forms into the database.**

The database is structured to reflect the format of the data collations forms to facilitate easy transfer of data from the forms into the database.

Once the coded data is entered the full text description is automatically displayed.

- **Analysing the data.**

Once the data has been verified and entered into the database it is analysed to determine three characteristics:

- Whether the fault is relevant or non-relevant.
- The total relevant downtime.
- The total non-relevant downtime.

The information required to determine the above is embedded within the database. Full instructions are defined in the guidelines

document and once the above has been completed the database can display the real time achieved availability of the system.

- **Preparing reports.**

Summary reports can be produced automatically from the database and these reports can be customised.

6 Lessons Learned from Practical Application

The principles described in this paper have been applied to implement RDT for electrical & mechanical systems installed in the recently constructed extensions to Athens Metro Lines 2 & 3. In this situation the responsibility for performing RDT lies with the construction joint venture (JV) that was responsible for the design and installation of the systems. The accepting authority is the owner of the Metro, Attiko Metro S.A. (AM).

The systems involved in the RDT exercise include:

- Tunnel ventilation, environmental control & HVAC
- Power remote control
- Fibre optic data transmission network
- Operational telephones
- Traction power supply equipment
- Auxiliary power supply equipment
- Lifts & escalators
- CCTV & PA systems

At the time of writing the RDT period for the extensions to line 2 (Sepolia to AG Antonios and Dafni to AG Dimitrios) and line 3 (Ethniki Amyra to D Plakendias) has been successfully completed.

The RDT period for the line 3 extension between Monistaraki and Egaleo has commenced and the same system will be implemented for a further extension to line 2 between AG Dimitrios and Elliniko with RDT planned to commence towards the end of 2009.

The FRACAS has proven to be successful and a number of salient points have arisen from the process of setting up and operating the system that have provided invaluable feedback ensuring its ultimate success.

Definition of testing

The importance of clear definition of the proposed testing through the detailed test plans has been demonstrated by a lengthy process of revision to these documents. A number of significant discrepancies between the understanding of the JV and the requirements of AM were identified and resolved. Only through this review process is it possible to ensure that all parties involved in the testing are satisfied with the proposals and will have confidence in (and hence will accept) the results.

An essential part of the overall process is to have clear definitions of exactly what constitutes unavailability of a system. From this the relevance or otherwise of all identified system failure modes can be determined, defined and ultimately coded and included in the database reference data.

It is the RDT test plans that define all of this and these documents form the basis of the whole exercise; agreement of all stakeholders as to the technical content of these documents is essential.

Without the clear prior definition of the information contained in the detailed test plans there is a significant risk that at the conclusion of the RDT period the accepting authority could reject results of the testing.

Organisation

The importance of understanding the actual organisational structure was emphasised by the role of the AM operation and maintenance organisation (AMEL). Although the JV were contractually responsible for the maintenance of the installed systems during the testing period, in reality AMEL staff performed most of the day-to-day fault investigation and corrective actions.

To address this a reporting process was devised whereby the existing procedures that are used by AMEL for fault reporting were integrated into the reporting process for the RDT thereby minimising the additional work required from AMEL staff and ensuring that the required information was recorded for the RDT.

The AMEL staff were also fully involved in the training process so that there was full understanding of the purpose of the testing and the information that is required to be recorded.

It was evident that the AMEL staff were initially sceptical of what they saw as an additional burden on their existing workload. However, once they understood the overall FRACAS process and why it was required and also saw that its implementation was structured in such a way as to compliment their existing responsibilities, they became supportive.

It is imperative that all parties involved in the implementation of the FRACAS understand what they are doing and why they are doing it.

Flexibility

The FRACAS has been designed to give a highly structured means of recording data to ensure consistency. However there is also need for flexibility in the system to allow for unforeseen circumstances. An example arose on the Athens RDT exercise whereby there was a significant delay to the repair of an escalator due to the lack of a maintenance contract. This delay was the fault of AM and therefore should not be included as relevant down-time of the escalator. Resolution of this situation was achieved by agreement between AM & JV and definition of the additional down time as non-relevant in the analysis such that the calculated availability of the escalator was not adversely affected.

There is provision in the database to allow the reasoning behind such decisions to be recorded and the process of approval of the test data by the accepting authority ensures that they are fully aware of the assumptions behind the analysis.

7 Summary

This paper presents a means to determine in-service availability of systems and equipment in a rigorous and consistent manner so that the predicted reliabilities and/or levels of safety can be assured. In this way the reliability performance can be established as part of an overall system condition monitoring programme.

In addition to validation of predicted system reliability performance, overall levels of safety can be improved by providing clear evidence to support reductions in the amount of intrusive maintenance activities. Ultimately it is possible to reduce ownership costs through optimising maintenance activities.

References

- [1] BS EN 50126 – Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
- [2] IEC 60300-3-5. Dependability Management – Application Guide – Reliability Test Conditions and Statistical Test Principles.
- [3] IEC 61124. Reliability Testing – Compliance Tests for Constant Failure Rate and Constant Failure Intensity.