DOCUMENT

Effective Reliability Prediction for Space Applications

White Paper

Prepared by	**TEC-QQD**
Reference	**ESA-TECQQD-WP-0969**
Issue	**1**
Revision	**3**
Date of Issue	**25/05/2016**
Status	
Document Type	
Distribution	

European Space Agency
Agence spatiale européenne

APPROVAL

Title Effective Reliability Prediction for Space Applications – White Paper	
Issue 1	**Revision** 3
Author TEC-QQD	**Date** 25.05.2016
Approved by TEC-QQ	**Date**

CHANGE LOG

Reason for change	**Issue**	**Revision**	**Date**
Initial release for internal review.	1	0	11/12/2015
Update following internal review.	1	1	01/04/2016
Update following working-level meeting with TEC-QQS.	1	2	21/04/2016
Update following TEC-QQ management review meeting.	1	3	25/05/2016

CHANGE RECORD

Issue	**Revision**		
Reason for change	**Date**	**Pages**	**Paragraph(s)**

Table of contents:

1. EXECUTIVE SUMMARY

This document describes the current situation in the reliability assessment process for space applications, highlights its inadequacies and limitations, and proposes corresponding improvements with a clear implementation strategy.

Reliability assessment is an end-to-end process beginning with the specification of system reliability. The system reliability requirement is then apportioned to the system constituents in a top-down fashion, down to the lowest functional level where reliability prediction is performed . The system reliability requirement is then verified with the help of reliability modelling techniques such as reliability block diagrams or simulation methods which take into account all of the lower level predictions. Reliability is a key input parameter for quantitative availability, maintainability and safety objectives and requirements.

Inadequacies and limitations in the current reliability prediction process have been highlighted [RD-30] such as arbitrary requirements specification, obsolete component failure rate modelling, overly-simplifying system modelling, and/or lack of test/field data utilisation. This results in a prediction that is inaccurate with respect to the system's in-orbit performance or demonstrated reliability leading to a potential over-design and consequently reduced cost effectiveness during the development process.

In order to correct the situation ESA suggests to improve the reliability assessment process. The improvements include a rationalisation of the quantitative reliability requirement specification process, an agreement on a unified framework to perform reliability prediction based on IEEE 1413, and the development or improvement of specific failure models for mechanical and electronic part types. In addition, in order to overcome the inherent limitations of the handbook-based prediction methods and in line with the principles of IEEE 1413, it is also recommended to pursue the enhancement of handbook-based reliability predictions with in-orbit/testing experience data through a Bayesian inference approach. The integration of other contributors to the system reliability such as software, human factors, systematic failures is to be studied. Nevertheless, the contribution of software, human factors and systematic failures to the system reliability is not discussed in detail in this paper.

The proposed implementation strategy is to structure the efforts in a logical manner following the steps of the reliability prediction process by making use of ESA's research and development (R&D) programs at TRP, GSP, and GSTP levels. To improve its effectiveness it is strongly recommended that the activities are coordinated with other stakeholders such as prime contractors and space agencies at national and international level. Coordination can be achieved by regular workshops such as AWARE/reliability workshop [RD-26] or jointly with key partners like NASA.

In response to the growing need for enhancing product reliability assessment in the increasingly competitive space industry, the goal of this activity is to improve the accuracy of reliability predictions and thus make them once again a powerful design tool that will help to increase the cost effectiveness of our satellite development programs.

2. BACKGROUND

Reliability is one of the key performance characteristics of a space system and its components which is continually evaluated throughout the development phase to ensure that the system provides its functionalities at a performance level sufficient to achieve the mission objectives. Several methods exist to predict reliability, including handbook based predictions, test data based predictions, and in-orbit or field data based predictions.

Handbook based predictions combined with reliability modelling techniques such as reliability block diagrams (RBD) are the most widely used method in space applications to evaluate the system reliability largely due to the lack of relevant field and/or test data.

The reliability predictions can be used for the following main purposes depicted in [Figure 2-1]:

- to establish whether a design meets/exceeds the system reliability requirement.
- to focus attention on weak parts/problem areas in the design.
- to assess the impact of design changes on system reliability.
- to compare competing designs or design alternatives.
- to determine the number and type of spare units for repairable systems.
- to support the system availability, repair, maintenance and lifecycle cost assessment.

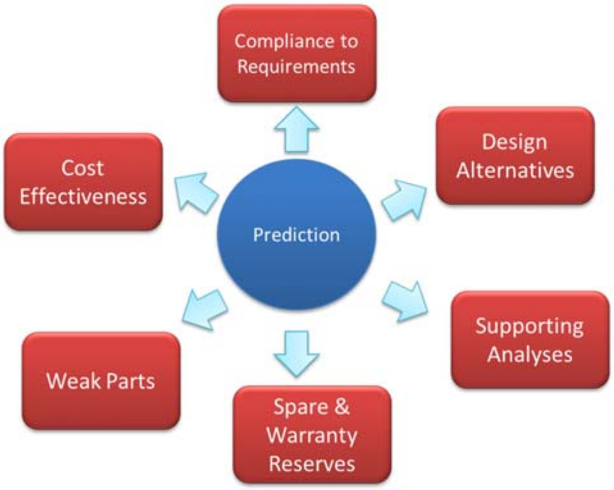


Figure 2-1: Reliability Prediction Uses

In order to be effective, the reliability prediction process has to overcome its current limitations/shortcomings such as:

- no clear criteria for the specification of quantitative requirements.
- simplified assumptions like constant failure rates.
- lack of statistical confidence.
- missing human factors or systematic failures (e.g. in design, manufacturing, etc.) which contribute to the unreliability of the system.
- use of models which are not complete or are outdated/obsolete with respect to technology evolution.
- limited use of relevant experimental data (test or field/in-orbit data) for support in the reliability prediction.

This paper proposes to properly account for all these elements in order to obtain a reliability prediction that is as accurate as reasonably possible with respect to the system's in-orbit performance or demonstrated reliability. In this respect, feedback from industry [RD-3] and academic research [RD-34]have highlighted that prediction results are largely conservative with respect to the actual in-orbit performance. This reassures the fully satisfactory operational suitability of the systems but at the same time gives the perception of potential over-design and consequently reduced cost effectiveness during the development process. It is to be noted that in some cases this in-orbit over-performance may be due to an under-stress use of a satellite during its operational lifetime as compared to the stress assumptions made to obtain the reliability prediction results during the design phase.

3. RELIABILITY MODELLING/PREDICTION END-TO-END PROCESS

The current reliability prediction and modelling end-to-end process for space applications is composed of the following steps:

- Specification of reliability requirement at system level
- Allocation of reliability requirements to lower levels (down to unit level)
- Verification of reliability specifications with reliability prediction at component level using handbook sources and supplier data (e.g. board level) followed by modelling at higher levels with reliability block diagrams (RBD) or simulation techniques (Monte Carlo, Markov, Bayesian networks, etc.)
- Potentially reliability predictions can be updated with test and or in-orbit data

The following chapters will expand on the above mentioned steps.

4. CURRENT PRACTICES IN THE RELIABILITY MODELLING/PREDICTION PROCESS

4.1 Specification of System Reliability

System reliability requirements provide the goals to ensure that the system will perform its intended function successfully for the specified period of time under the given operating environment. Reliability requirements tend to be more stringent for safety critical, long duration, or high cost/visibility missions, and more relaxed or inexistent for low cost or short duration missions. In the case of low cost/short duration missions, reliability is considered to be assured in most cases only by the identification and elimination of critical areas such as single point failures and the use of space-grade components [RD-27] when compatible with the project constraints e.g. budget.

Reliability requirements are usually specified at satellite level in the form of a probability of success at end of life without specifying any confidence level. Nevertheless, depending on the needs of the project the quantitative reliability requirements may also be specified at mission level (including ground and launch segments) or at space segment/system level. Other reliability metrics may include:

- Mean life: Average or expected time to failure. It is denoted as mean time to failure (MTTF) for non-repairable systems and mean time between failures (MTBF) for repairable systems. These terms are generally used under the assumption that the failure distribution is exponential and thus the failure rate is constant.
- Failure rate: Reciprocal of the mean life for constant failure rate. It represents the number of failures per unit time (failure frequency) at a given age.

Quantitative reliability specifications across different European Space Agency projects at satellite level are provided in [Figure 4-1]:

Project	Directorate (purpose)	Specified Lifetime	Satellite Reliability Specification	Reference
Cryosat 2	Earth Observation (investigation of Ice Polar Regions)	3.5 years including commissioning and validation.	The success probability of 70% or better is required for nominal performance for the overall mission time.	CS-RS-ESA-SY-0006 (SRD)
GOCE	Earth Observation (gravity field)	20 months	No quantitative reliability specification (A reliability target was derived from an availability requirement by the prime)	GO-RS-ESA-SY-0002 (SRD)
Mars Express	Science (investigation of Mars)	1610 days (extended)	No quantitative reliability specification	MEX-EST-RS-2003
Meteosat Second Generation	Earth Observation, (weather)	7 years	The specified reliability figure is 0.68 for a 7 years in orbit mission.	MSG.ASC.SA.SY>0075
Meteosat Third Generation (MTG)	Earth Observation (weather)	8.5 years following a maximum on-ground storage of 10 years	• **SA-REL-010**: Regarding the FCI mission, the reliability of the MTG-I satellite shall be higher than 0.75 at the end of the satellite specified lifetime. • **SA-REL-020**: Regarding the LI mission, the reliability of the MTG-I satellite shall be higher than 0.75 at the end of the satellite specified lifetime. • **SA-REL-030**: Regarding the Data Collection System (DCS) mission, the	MTG.ESA.SA.RS.0062 (SRD)

Project	Directorate (purpose)	Specified Lifetime	Satellite Reliability Specification	Reference
			reliability of the MTG-I satellite shall be higher than 0.90 at the end of the satellite specified lifetime. • **SA-REL-040**: Regarding the IRS mission, the reliability of the MTG-S satellite shall be higher than 0.75 at the end of the satellite specified lifetime. • **SA-REL-050:** The reliability of the MTG platform shall be higher than 0.917 at the end of the satellite specified lifetime.	
Rosetta	Science (investigation of a comet)	3888 days	The reliability target for the Rosetta avionics is given equal to 0.93 for a mission duration of 11 years (3888 days).	RO.DSS.RS.2001
Sentinel 1	Earth Observation	7 years after a maximum on-ground storage of 10 years.	• **PAS-004** :The Platform shall provide the nominal required support to the Payload instrument with a probability better than 0.80 over the specified life, including the launch phase. • **PAS-005**: The Payload instrument shall provide a nominal performance with a probability better than 0.85 over the specified life.	S1-RS-ESA-SY-0001 (SRD)
Sentinel 2	Earth Observation	7 years after a maximum on-ground storage of 10 years and following the LEOP and commissioning phase.	• **SAT-REL-005**: The satellite overall reliability shall be better than 0.70 over the specified lifetime.	S2-RS-ESA-SY-0001 (SRD)
Sentinel 3	Earth Observation	7 years after a maximum on-ground storage of 10 years and following the in-orbit commissioning.	• **SA-RE-010**: The reliability of the platform shall be better than 0.90 over the specified lifetime. • **SA-RE-020:** The reliability of the platform combined with the reliability of anyone of the main instruments (or group of instruments in the case of Topography) shall be better than 0.75 over the specified lifetime.	S3-RS-ESA-SY-0010 (SRD)
Seosat	Earth Observation	7 year (after commissioning)	• **SY-PER-400**: The total reliability of the space segment shall be better than 65 %.	SEOS-RS-ESA-SY-0002 (SRD)
Solar Orbiter	Science (investigation of the Sun)	10.2 years	No quantitative reliability specification	SOL-EST-RS-1717
SWARM	Earth Observation (geomagnetic field)	4 year	• **GSR-3**: Reliability is defined as the probability that each satellite (platform + payload) will carry out its specified mission for the specified total operational lifetime Each Swarm satellite shall be designed to provide a reliability of higher than 0.8 over the total operational lifetime.	SW-RS-ESA-SY-001 (SRD)
VEGA	Launcher	Per mission.	• **6.7.1.1**: The probability of Vega failing to complete its mission in compliance with the requirements of this document, due to failure or malfunction of any component, after the pre- flight check out and up to the end of the collision avoidance manoeuvre, shall not exceed 2 .10-2 (mission reliability of 0.98 with a confidence level of 60%).	VG-ESA-SP-001 (SRD)

Figure 4-1: Reliability Specifications in Several European Space Agency Projects

4.2 Reliability Allocation to Lower Levels

Reliability requirements are allocated or apportioned from system level (e.g. satellite) to all subsystems. Then in turn each subsystem apportions its reliability requirement to each unit or equipment. If each unit achieves its allocated reliability then the subsystem will meet its requirement, and if all subsystems meet their requirements then the system will meet its system level reliability requirement.

A necessary prerequisite for the allocation is to have a system breakdown in the form of a reliability block diagram. There are then several methods to allocate system reliability requirements to lower levels:

- Equal allocation that assigns to each subsystem/unit an equal part of the system reliability requirement.
- Weighted allocation (e.g. ARINC Allocation method, bottom-up allocation) that takes into account the complexity of the subsystem and any prior information available (e.g. available failure rates).

The allocation process is iterative. As more design information becomes available the system and subsystem teams may update the various allocations to the subsystems or units in order to meet the overall system reliability requirement.

4.3 Component Reliability Prediction

Once the initial reliability allocation process to lower levels has been completed it is time to determine whether the established reliability targets are met at all design levels from component to unit, to subsystem, to system level. In space applications components are for the most part electrical/electronic although there is also a substantial amount of mechanical components. Other integral system elements which are contributors to the reliability of the system, such as structural components or software, are currently dealt with through e.g. margins of safety/factors of safety or software assurance processes. Indeed reliability analyses such as FTA and FMECA were developed to cope with random wear-out failures in hardware and are not very effective against design errors [RD-14].

The most widely used method for reliability prediction of electrical/electronic systems across all industrial sectors including space is the handbook based MIL-HDBK-217. The standard assumes that electronics can be modelled using a constant failure rate and contains failure rate data for passive (e.g. resistors, inductors, capacitors, etc.) and active components (transistors, diodes, integrated circuits, etc.). There are methods to adjust the base failure rate of the components depending on the use environment, quality control requirements, the number of gates in an integrated circuit, etc. The factors used to modify the base failure rate are known as π factors. There are two main prediction methods within MIL-217, the parts count and the parts stress method. The parts count method assumes an average stress level as a way to provide an early design estimate of the component failure rate whereas the parts stress method requires the knowledge of the stress levels experienced by the component. A circuit board failure rate is then predicted by adding the failure rates of all the parts mounted on the board. This assumes a series model (i.e. no internal redundancy) for the circuit board and will result in a worst case prediction. Since a series model is assumed , the resulting failure rate of the system is constant given that all the components of the system have a constant failure rate.

Other handbook prediction methods for electronics such as PRISM were developed to overcome some of the inherent limitations of MIL-HDBK-217 which is no longer being maintained. PRISM incorporates a system level failure rate model, new component type models, and the ability to use field and test data in the prediction among other improvements. Likewise another methodology, 217Plus, expands PRISM by including new part type failure rate models and combining them with experience data using the Bayesian update approach. A comparison between predicted reliability using MIL-HDBK-217 and PRISM/217Plus versus observed reliability for military equipment is provided in [Figure 4-2].

Another handbook based reliability prediction methodology for electronics that is gaining momentum in Europe is FIDES [RD-5] which is intended to predict realistic reliability values close to the average[1] values usually observed in the field. It does so by modelling not only the physical/technological contributions to failure but also the process contributions e.g. the effects of the development, production and operation processes on reliability as depicted in [Figure 4-3].

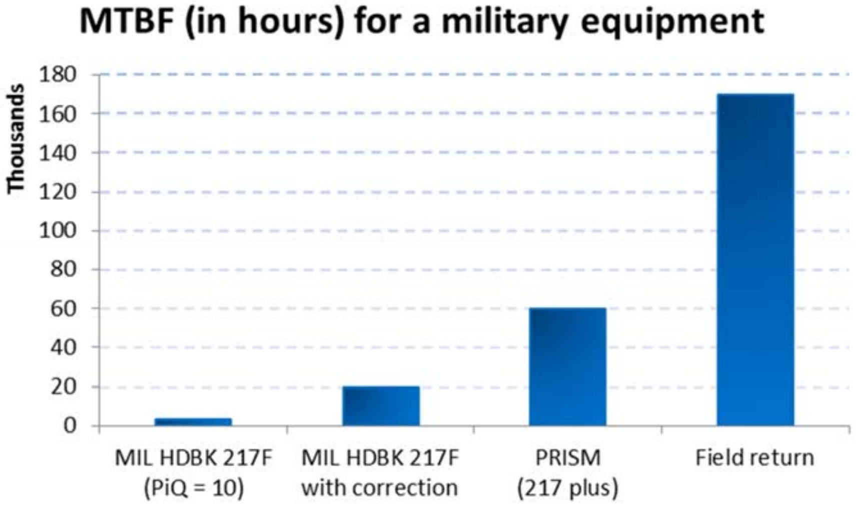


Figure 4-2: Comparison between Predicted and Observed Reliability

[1] The failure rate models the average occurrence rate of a failure as this is the meaning of the parameter as used in the exponential law. This represents the flat part of the failure rate bathtub curve which is the usual considered assumption in reliability prediction of electronic equipment.

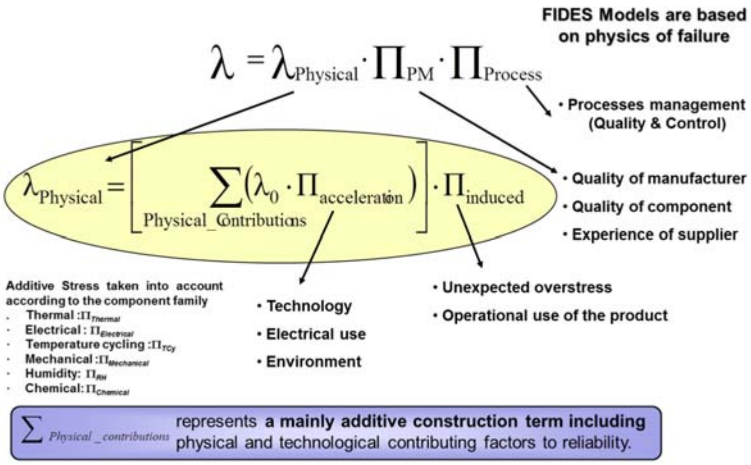

FIDES Models are based on physics of failure
$\lambda = \lambda_{Physical} \cdot \Pi_{PM} \cdot \Pi_{Process}$
• Processes management (Quality & Control)
$\lambda_{Physical} = \left[\sum_{Physical\_Contributions} (\lambda_0 \cdot \Pi_{acceleration}) \right] \cdot \Pi_{induced}$
• Quality of manufacturer
• Quality of component
• Experience of supplier
Additive Stress taken into account according to the component family
Thermal : $\Pi_{Thermal}$
Electrical : $\Pi_{Electrical}$
Temperature cycling : Π_{TCy}
Mechanical : $\Pi_{Mechanical}$
Humidity: Π_{RH}
Chemical: $\Pi_{Chemical}$
• Technology
• Electrical use
• Environment
• Unexpected overstress
• Operational use of the product
$\sum_{Physical\_contributions}$ represents a mainly additive construction term including physical and technological contributing factors to reliability.

Figure 4-3: FIDES Global Model

In space systems we encounter in addition to electronic systems many mechanical systems and components. For those kinds of components there are handbooks available such as NSWC-11 Handbook of Reliability Prediction Procedures for Mechanical Equipment. The handbook is similar in format to MIL-HDBK-217 and includes base failure rates of mechanical components which can be adapted by c factors depending on the type of material properties, the system operating environment, etc. Some of the specific systems covered by the standard include seals and gaskets, springs, valves, bearings, motors, and other mechanical equipment. Similarly to MIL-HDBK-217, the NSWC-11 also assumes a constant failure rate model. Other sources of mechanical parts failure rates include NPRD-2011 (Non-electronic Parts Reliability Data) which allows to take into account wear out failures.

For completeness, ECSS-Q-HB-30-08A, “components reliability data sources and their use”, identifies suitable data sources and corresponding handbook methods that can be used for reliability prediction of components in space applications.

4.3.1 Limitations of Handbook-based Predictions

Handbook based reliability predictions have certain limitations. The most clear simplification is the underlying assumption that the components have an intrinsic constant failure rate while it has been shown experimentally that at the microscopic level very few failure mechanisms show this type of behaviour. Nevertheless, it is still a valid simplifying assumption when considering cumulative failure mechanisms across multiple and varied component types. Another simplification is the series system assumption where the predicted failure rate of a circuit board results from the sum of the predicted failure rates of all the components on the board which leads to a worst-case (conservative) prediction.

In addition, a handbook-based reliability prediction does not generally provide statistical confidence since there is no relevant experimental data for support. This is due to the disjointed nature of the data sources used in the development of the component models.

Furthermore, most handbook based predictions do not account for physics or mechanics of failure nor systematic failures. There is also an over emphasis on temperature as the key factor in electronic part failure while other issues such as temperature cycling, humidity, vibration, shock are not modelled. In addition, predictions only account for a small percentage of field failures related to part failures while most field failures originate from systematic failures in design, manufacturing or testing processes [RD-31].

Finally, MIL-HDBK-217, the most widely used prediction handbook is obsolete as it was last updated in 1995 and does not cover new components, technology advancements and quality improvements. Industry is applying corrective factors when sufficient in-orbit data exists (e.g. battery cells, solar cells, etc.) and developing models for new technologies (e.g. highly integrated circuits) but these efforts are not consolidated at European level leading to inconsistencies across various suppliers.

Nevertheless, it is to be noted that handbooks such as 217Plus and FIDES have developed strategies to cope with the limitations of MIL-HDBK-217, as depicted in [Figure 4-4] for the case of FIDES.

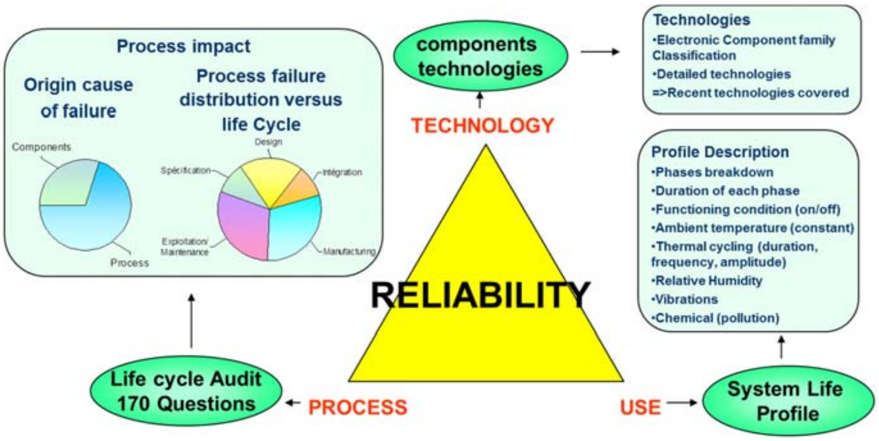


Figure 4-4: FIDES Approach to Overcome Limitations of Handbook-Based Predictions

4.3.2 Other Component Prediction Methods

Other component prediction methods include those that make use of available test data. Reliability predictions can be made based on the parameters of the probability distribution that fits the available time-to-failure data. The most widely used distribution is the Weibull because of its versatility to take different shapes and model each of the stages in the life of a product [Figure 4-5]:

- Early Life: Decrease in failure rate. Weibull beta parameter less than 1
- Useful life: Constant failure rate. Weibull beta parameter equal to 1, becomes the exponential distribution
- Wear-out: Increase in failure rate. Weibull beta parameter greater than 1

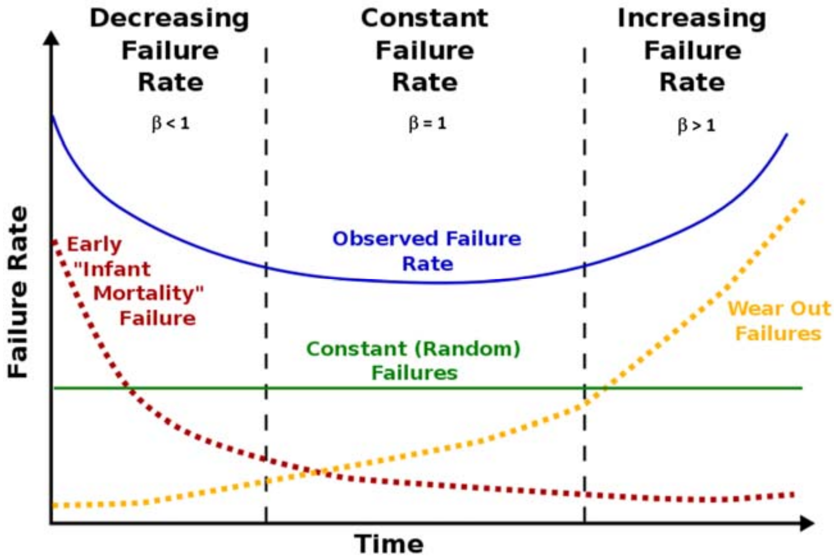


Figure 4-5: Weibull Beta Parameter to Model Each Life Stage of a Product

It is important to stress that the only current reliability prediction methods that can be used to actually estimate the reliability are those that make use of the relevant test or field data. Predictions that do not make use of relevant field and/or test data should be employed for other purposes such as to help focus attention on weak parts/problem areas in the design, assess the impact of design changes on system reliability or compare competing designs or design alternatives.

Finally, the physics-of-failure approach to system reliability is gaining momentum. It focuses on the mathematical modelling of the actual failure mechanisms to generate performance indications and reliability predictions.

4.4 System Reliability Prediction

Several methods exist to derive system reliability from component reliability. The two main approaches are:

- Reliability block diagrams (RBD), see [Figure 4-6].
- Simulation models (Monte Carlo, Bayesian Networks, etc.).

RBDs are the most popular method for system reliability analysis in space applications because of their relative ease of use and simple formulas under the assumption that the system blocks have constant failure rates (exponential distribution). RBDs break down the system into its constituent subsystems, units, and components represented by functional blocks. The effect of the failure of each block on the system is then evaluated using the reliability block diagram technique. System reliability models can be static (series, parallel, k out of n, etc.) or dynamic (load sharing, stand-by).There are several advantages to modelling systems with RBDs in addition to predicting system reliability, such as helping to assess the reliability impact of changes to the system, identifying major unreliability contributors thus pin pointing where reliability improvement activities should take place.

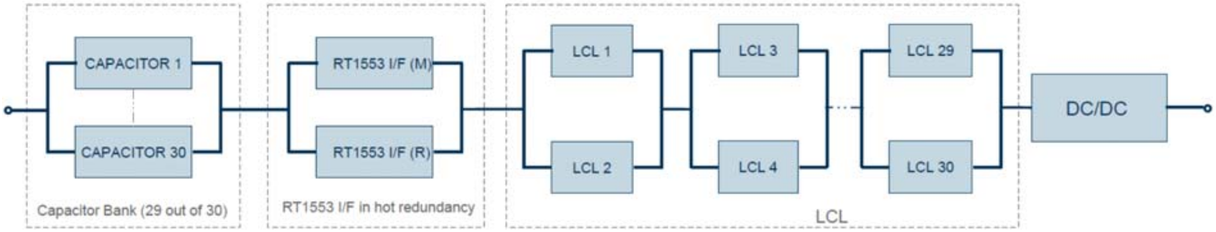


Figure 4-6: Example of a Reliability Block diagram for an Electrical Power Supply Unit

Simulation based models are used to model complex dynamic systems made up of blocks which may be dependent on failure distributions other than the exponential. Simulation based methods also allow to compute other reliability related metrics such as availability (e.g. with Markov chains [Figure 4-7] or Petri nets [Figure 4-8]).

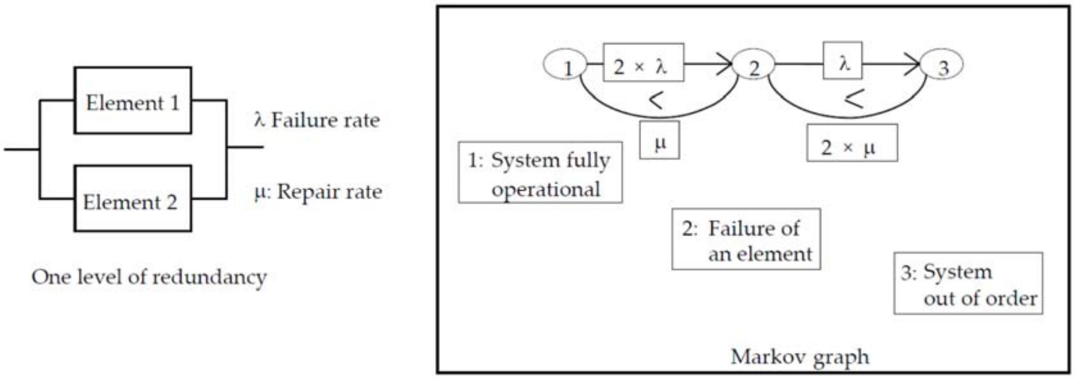


Figure 4-7: Example of Markov Graph

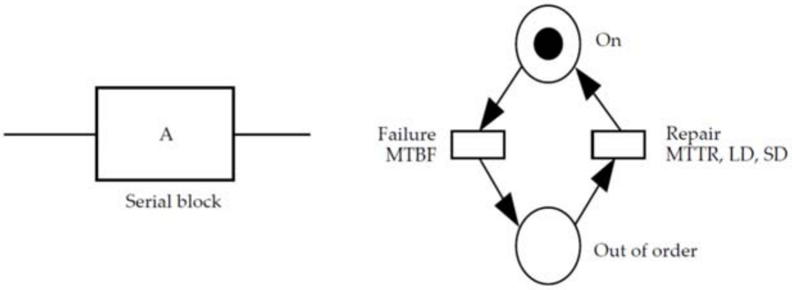


Figure 4-8: Example of Petri Net Used in Monte-Carlo Simulation

4.4.1 System Reliability Prediction vs. Field/In-Orbit Reliability

In the space domain it is widely accepted that predictions made with MIL-HDBK-217 are in general conservative, meaning that the product will have a failure rate which is less than the predicted value.

In fact, this statement has been verified in recent years when reliability predictions at satellite level have been shown to be significantly lower (although within the lower two-sided 95% confidence bound) than reliability estimations based on in-orbit data to the point where the usefulness of the current reliability prediction method has been questioned by Industry [RD-4].

Also in military applications the use of reliability predictions has produced misleading and inaccurate results [RD-20] although, contrary to space, the experience with military systems has shown that field reliability is lower than predicted (i.e. MIL-HDBK predictions are too optimistic).

The introduction of adjustment factors for MIL-HDBK-217 failure rates [RD-3] (see Figure 4-9) and/or the use of complementary methods (e.g. Bayesian update [Figure 4-10] with in-orbit feedback [RD-25]) have been suggested to resolve the so called inaccuracies of the predictions.

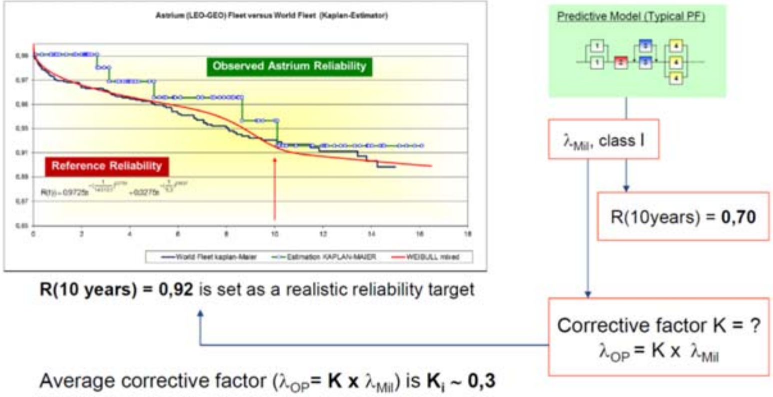


Figure 4-9: Adjustment Factors for MIL-HDBK-217 Failure Rates

The approach of adjusting MIL-HDBK-217F failure rate figures by means of corrective factor extrapolated from in orbit fleet data was reviewed by ESA [RD-22]. It was concluded that the variability of the population characteristics and the limited sample size made it difficult to define a statistically sound corrective factor to be applied for future programs. It was therefore not recommended at the time to use the methodology presented in [RD-22]to verify compliance to reliability requirements.

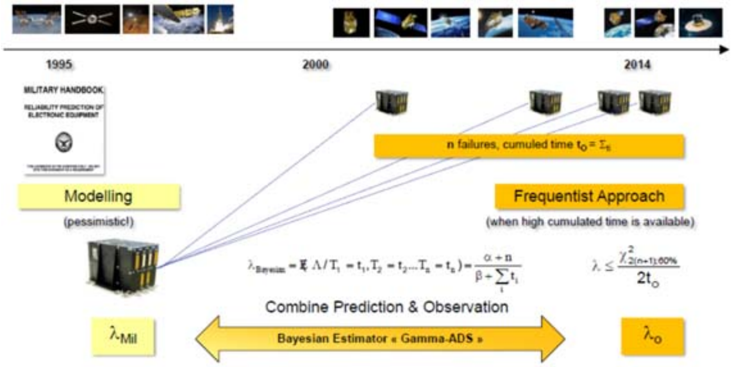

1995
2000
2014
MILITARY HANDBOOK
RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT
n failures, cumuled time $t_O = \Sigma_t$
Modelling
(pessimistic!)
Frequentist Approach
(when high cumulated time is available)
$\lambda_{Bayesian} = E(\Lambda / T_1 = t_1, T_2 = t_2 ... T_n = t_n) = \frac{\alpha + n}{\beta + \sum_i t_i}$
$\lambda \leq \frac{\chi^2_{2(n+1);60\%}}{2t_O}$
Combine Prediction & Observation
λ_{Mil}
Bayesian Estimator « Gamma-ADS »
λ_O

Figure 4-10: In-Orbit Bayesian Estimator "Gamma-ADS"

4.4.2 *Missing Factors in Current System Reliability Prediction*

One of the apparent reasons of why current reliability predictions are not in-line with actual in-orbit demonstrated reliability is because not all contributors [Figure 4-11] to system reliability are being properly considered. Current system reliability predictions cover only random failures when it has been shown [RD-29] that many of the experienced anomalies in-orbit are due to other than random causes such as design, manufacturing, or wear out. Other factors like software or human involvement (operators, manufacturing/testing technicians, etc.) play a major role in system reliability but are also not covered by the widely used prediction methods in space applications.

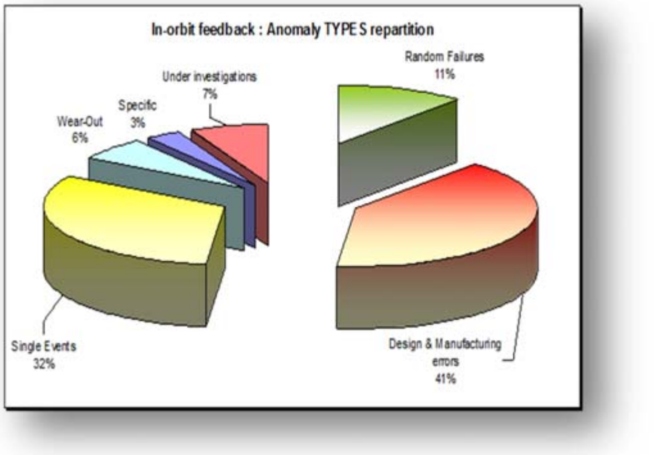
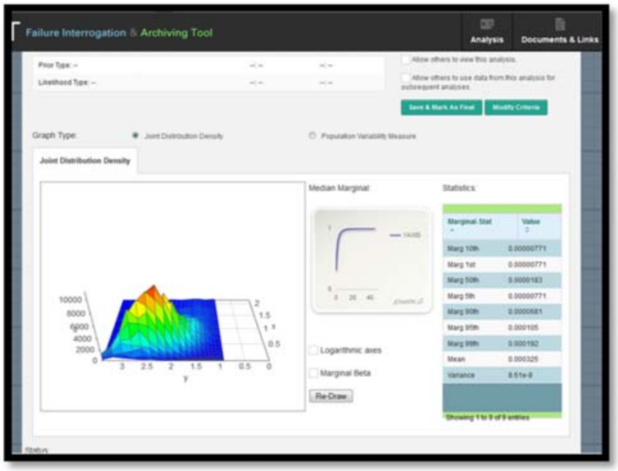


Figure 4-11: RAMS In-Orbit Data Exploitation (RIDE) Anomaly Root Cause Repartition

In addition, there is no extended use of relevant test and or field data that could complement the prediction to turn handbook-based predictions into actual reliability estimates.

4.5 Reliability Prediction Update from Test and Field Data

As more relevant field data becomes available from the failure data exploitation of in orbit experience, reliability models can be improved by including this additional data and turning reliability predictions into more accurate reliability estimates in-line with in-orbit experience. This can be achieved at all system levels using Bayesian inference. The approach [Figure 4-12] is currently being implemented in NASA with the help of tools like FIAT [RD-25].



Prior Type: --

Likelihood Type: --

□ Allow others to view this analysis.

□ Allow others to use data from this analysis for subsequent analyses.

Graph Type: ● Joint Distribution Density ○ Population Variability Measure

□ Logarithmic axes

□ Marginal Beta

Marginal-Stat	Value
Marg 10th	0.00000771
Marg 1st	0.00000771
Marg 50th	0.0000183
Marg 5th	0.00000771
Marg 90th	0.0000681
Marg 95th	0.000105
Marg 99th	0.000182
Mean	0.000325
Variance	8.51e-8

Showing 1 to 9 of 9 entries

Figure 4-12: FIAT Generated Likelihood Function for Posterior-to-Prior Conversion – Bayesian Learning

However, the approach has to take into account the differences in the in-orbit satellite attribute input data with respect to the system under consideration, i.e. differences in the architecture, the technologies, the environment, operation and lifetime.

5. PROPOSED IMPROVEMENTS FOR SPACE APPLICATIONS

5.1 Rationalising the Specification of Reliability Requirements

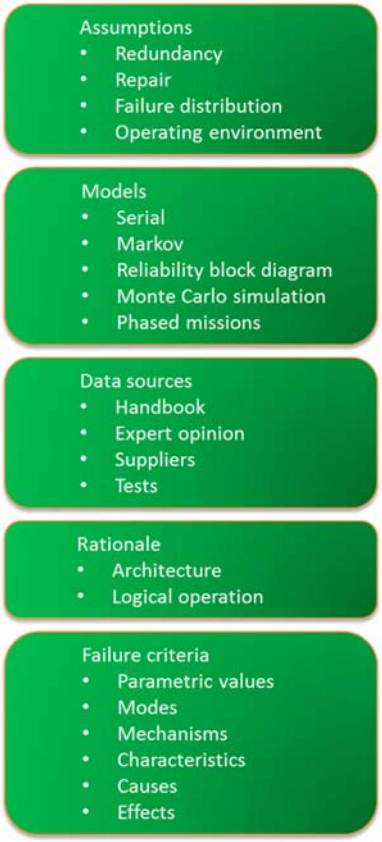
Reliability requirements are to be specified according to a pre-defined criteria. This criteria should be based on customer needs, the mission objectives, priority/visibility/significance to the Agency, or mission cost. At the time of writing there is an ongoing activity [RD-28] to identify a systematic criteria for the definition and application of quantitative reliability requirements to future ESA space programs and to establish a methodology to effectively define appropriate metrics, apportion and flow-down quantitative requirements with respect to mission/program success criteria (e.g. mission objectives).

5.2 Agreeing on a Unified Framework for Reliability Prediction

In order to have credible outputs from the reliability prediction process it is recommended to establish a unified framework for reliability predictions activities such that prediction results are better understood and their use in line with the purposes described in the background section of this white paper.

The framework would allow the identification of existing reliability prediction methods that can be selected as needed during design and development (e.g. Handbook-based, physics-of-failure based, test/field data based, etc.).

In addition, the framework would ensure that information [Figure 5-1] regarding inputs, assumptions, data sources, used methodologies/limitations, and uncertainties is properly addressed such that the risk associated in using the prediction is identified and reported for customer approval.



Assumptions
- Redundancy
- Repair
- Failure distribution
- Operating environment

Models
- Serial
- Markov
- Reliability block diagram
- Monte Carlo simulation
- Phased missions

Data sources
- Handbook
- Expert opinion
- Suppliers
- Tests

Rationale
- Architecture
- Logical operation

Failure criteria
- Parametric values
- Modes
- Mechanisms
- Characteristics
- Causes
- Effects

Figure 5-1: Prediction Attributes to be Documented as Recommended in IEEE1413

To this end the IEEE 1413 standard [RD-11] is recommended.

The IEEE 1413 is not a reliability prediction method and it does not replace or supplement any available prediction method. The standard also does not recommend or prohibit the use of any particular reliability prediction method. A prediction made according to IEEE 1413 ensures that the benefits and limitations of a prediction method is considered and evaluated by the engineers preparing the prediction and that the users of the prediction are aware of the same. This standard elevates the process of reliability prediction from a time routine and obligatory task to a value added activity [RD-18].

Unless a new and more suitable prediction method for space will be developed in the short term, and its consistency validated by consensus among the European community of practitioners (Industry, Agencies and Academia), none of the existing standards can be

considered optimum for all situations and the approach should not prescribe any particular methodology to follow. In the long term, ESA intends to identify a suitable methodology to be applied by all industrial partners.
Nevertheless, the most relevant methodologies today for space applications include 217Plus, FIDES, and life testing (only at lower levels, if practical).

A particular failure rate data source shall be chosen depending on the operating conditions and the operating environment that best reflects the end application.

The following points should be taken into account when deciding which methodology to use:

- To be as much realistic as possible with respect to the stresses experienced in operation but also throughout other project phases (e.g. manufacturing, testing, handling, etc.) in terms of mechanical, chemical, thermal and electrical stresses.
- Allow the assessment of the various processes during the development phases (design, manufacturing, testing, etc.) , i.e. non part related failure causes.
- Consider operating and non-operating phases and cycles.
- Define on the basis of physics-of-failure principles.
- Applicability to wide applications and part types (specific and COTS).
- Combining relevant test and/or in-orbit experience data.

The technical data to be included in a systematic reliability prediction report document shall include at least the following:

- Uncertainties and limitations on the prediction
- Statistical confidence in the prediction

As described in IEEE Std 1413, the usefulness of a reliability prediction is based on how the prediction is developed and how well the prediction is prepared, interpreted, and applied.

5.3 Developing a New Reliability Prediction Methodology

Reliability predictions are impacted by the accuracy and completeness[2] of the information provided to perform the prediction and the methods used to complete the prediction.
For this purpose, the collaborative study (TEC-Q, TIA-T, TEC-E) on enhanced reliability prediction methodologies is proposed. The study should help fill the gap with respect to existing component failure models and develop failure models for new (critical) components like complex integrated circuits for which reliable models do not exist or are not standardized across industrial space companies. The models shall cover both mechanical and electronic components and may be based on physics-of-failure or field/test data. The failure models shall address additional factors such as operating and non/operating periods and cycles and wear-out. It is to be assessed whether the new

[2] The level of information accuracy and completeness will be assessed during the course of R&D activities

methodology could also include non-part related/systematic failure causes (like manufacturing defects), human factors, and software.
In addition, in order to overcome the inherent limitations of the handbook-based prediction methods and in line with the principles of IEEE 1413, it is also recommended to pursue the enhancement of handbook-based reliability predictions with in-orbit/testing experience data through a Bayesian inference approach.

5.4 Upgrading Standards and Handbooks

At this time, there are several reliability-related studies which were proposed to solve the limitations of the current reliability prediction methodology in space applications, namely, quantitative reliability requirements , reliability data sources, mechanical reliability prediction, and enhanced reliability prediction methodology. Details of these studies can be found in chapter 10. Once completed in 2016, it is expected that their consolidated conclusions may be proposed to be incorporated into the existing ECSS reliability standards [RD-1] and handbooks [RD-2]. In addition, an ECSS dedicated reliability prediction handbook is strongly recommended.
These activities will have to be implemented in coordination with other stakeholders with a clear implementation strategy.

5.5 Reinforcing the Practices to Evaluate Reliability Capability

Assessments are highly recommended to evaluate the supplier's reliability capability and to evaluate the adequacy of their reliability program plans. In particular, when new technology products / parts are under development, assessments are beneficial to early identify the suitable design analyses required to give the customer confidence in the product, and the supplier the necessary understanding to introduce design changes in a cost-effective manner.

Assessments are also intended to support industry to assess their efforts to maintain the required academic knowledge, whilst bringing the competences up-to-date with the latest reliability methodologies and practices.

For this purpose a suitable tool for conducting the assessment would be useful and needs to be identified (e.g. the AMSAA Reliability Scorecard tool [Figure 5-2], [RD-32]).

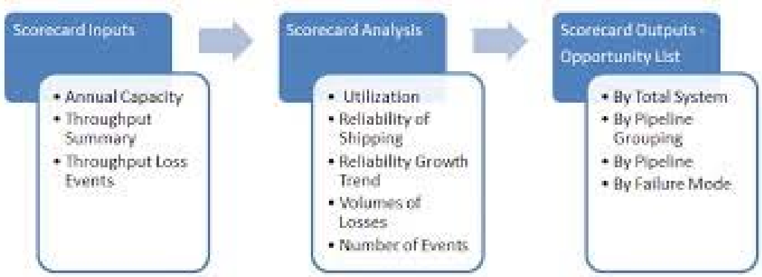


Figure 5-2: Scorecard Process

6. IMPLEMENTATION STRATEGY

The proposed implementation strategy for the improvement of reliability prediction in space applications is to structure the efforts in a logical manner following the steps of the reliability prediction process by making use of ESA's core research and development (R&D) programs at TRP,GSP and GSTP levels following the TEC-QQD technology roadmap [RD-33]. To improve effectiveness it is strongly recommended that the activities are coordinated with other stakeholders such as prime contractors and space agencies at national and international level. Coordination can be achieved by regular workshops such as AWARE/reliability workshop or jointly with key partners like NASA.

7. CONCLUSIONS

This document described the current situation in the end-to-end reliability prediction process for space applications, highlighted some of its inadequacies and limitations, and proposed corresponding improvements with a clear implementation strategy.

It has been explained that current inaccuracies in the predictions are mostly due to the multiple weaknesses in the process, from arbitrary requirements specification, to obsolete component failure rate modelling, to overly-simplifying system modelling, and lack of test/field data utilisation.

In order to improve the situation, ESA is making suggestions geared towards a more accurate (as reasonably as possible) reliability prediction process that will establish reliability prediction once again as a powerful design tool that will help to increase the cost effectiveness of our satellite development programs. The improvements include a rationalisation of the quantitative reliability requirement specification process, an agreement on a unified framework to perform reliability prediction based on IEEE 1413, and the development or improvement of specific failure models for mechanical and electronic part types for which data availability will be the greatest challenge . In addition, in order to overcome the inherent limitations of the handbook-based prediction methods and in line with the principles of IEEE 1413, it is also recommended to pursue the enhancement of handbook-based reliability predictions with in-orbit/testing experience data through a Bayesian inference approach. The integration of other contributors to the system reliability such as systematic failures is to be studied. This is to be achieved following a clear implementation strategy firmly based in ESA's core R&D plans in cooperation with other Agency partners and industrial stakeholders.

8. BIBLIOGRAPHY

RD-1 ECSS-Q-ST-30C, Dependability , 2009

RD-2 ECSS-Q-HB-30-08, Components data sources and their use, 2011

RD-3 Gajewski, Satellite reliability based on in-orbit feedback, 2013

RD-4 Gajewski, A Status on Complex Parts Reliability Assessment, 2014

RD-5 FIDES Guide 2009, Edition A, Reliability Methodology for Electronic Systems, 2010

RD-6 ANSI/VITA 51.1-2008, Reliability Prediction MIL-HDBK-217 Subsidiary Specification

RD-7 ANSI/VITA 51.2-2011, Physics of Failure (PoF) Reliability Predictions

RD-8 Nicholls, D., System Reliability Toolkit, Reliability Information Analysis Center (RIAC), 2005

RD-9 MIL-HDBK-217F, Reliability Prediction of Electronic Equipment

RD-10 MIL-HDBK-338B, Military Handbook: Electronic Reliability Design Handbook

RD-11 IEEE Std 1413™-2010, IEEE Standard Framework for Reliability Prediction of Hardware

RD-12 IEEE Std 1332™-2012, IEEE Standard Reliability Program for the Development and Production of Electronic Products

RD-13 DOD Guide for Achieving Reliability Availability and Maintainability (RAM), 2005

RD-14 Leveson, N. G., Course on System Safety for Software-Intensive Systems ESA ESTEC (5-8 Nov 2007)

RD-15 McLeish, J. G., Enhancing MIL-HDBK-217 Reliability Predictions with Physics of Failure Methods

RD-16 O'Connor, P., Practical Reliability Engineering, 5th Edition, Wiley

RD-17 Nicholls, D., An Objective Look at Predictions – Ask Questions, Challenge Answers, Reliability Information Analysis Center (RIAC), IEEE-RAMS, 2012

RD-18 Pecht, M., et al., The IEEE standards on reliability program and reliability prediction methods for electronic equipment

RD-19 Elerath, J.G.,Pecht, M., IEEE 1413: A standard for Reliability Predictions

RD-20 Jais, C., Werner, B., Das, D., Reliability Predictions – Continued Reliance on a Misleading Approach

RD-21 Morris, S. F., Rome Lab. MIL-HDBK-217 A favorited target.

RD-22 Operational Reliability Approach by Astrium - ESA Assessment, TEC-QQD-TN-01.04

RD-23 Reliability Prediction Data Sources and Methodologies for Space Application, ESA-TECQQD-SOW-0406, 2014

RD-24 Benbow, D. and Broome, H. W., The Certified Reliability Engineer Handbook, 2 ed. ASQ Quality Press. 2013.

RD-25 Lindsey, N., Brall, A., Mosleh, A., Reliability Prediction Using Bayesian Updating of On-Orbit Performance, AIAA RAMS 2013

RD-26 Reliability Assessment Initiative (AWARE Workshops)

RD-27 Current Practices in the Use of Quantitative Reliability Requirements in Space and Non-Space Applications, TN1, AKKA Technologies, 2015

RD-28 Use of Quantitative Reliability Requirements for Space Applications, ESA-TECQQD-SOW-0405, 2014

RD-29 RAMS Exploitation of In-orbit Data, Contract ESTEC 21167/07/NL/EM

RD-30 TEC-Q Reliability WG -Report on Gaps and Possible Solutions for Reliability Prediction, Issue 1, 7/7/2011

RD-31 Reliability Modelling, The RIAC Guide to Reliability Prediction, Assessment, and Estimation, RIAC

RD-32 Marguerite H. Shepler, N. Welliver, USAMSAA, New Army and DoD Reliability Scorecard

RD-33 Safety & Dependability R&D Roadmap –SDRM, Issue 1.1, 03/06/2013, ESA-TEC-QQD-TN-1683

RD-34 Castet, J. F., Saleh, J. H., , Hiriart, T., Lafleur, J.M., Comparative Reliability of GEO, LEO, and MEO Satellites, IAC-09.D1.6.1, 2009

9. ANNEX A: POTENTIAL DATA SOURCES (FROM ECSS-Q-HB-30-08A)

9.1 Introduction

This Annex provides information to the user concerning data sources for component failure rate determination. This list is not comprehensive, and is not intended to give a preference for sources. It remains up to the user to determine which data source is relevant for the application. Data sources in this Annex stem from ECSS-Q-HB-30-08A. Since its publication, several data sources have been revised and updated. For the latest versions, the user may refer to commercially available reliability support tools.

9.2 EEE Parts

9.2.1 AT&T Reliability Manual

The AT&T reliability manual is more than just a prediction methodology. Although it outlines prediction models and contains component failure data the book also describes the AT&T approach to reliability and covers many diverse reliability topics, albeit with a bias towards reliability prediction. The main prediction models are based on a decreasing hazard rate model, which is modelled using Weibull data. In this respect the handbook is unique.

9.2.2 FIDES (UTE C 80-811)

FIDES is a new reliability data handbook (available since January 2004) developed by a consortium of French industry under the supervision of the French DoD (DGA).

The FIDES methodology is based on physics of failures and is supported by the analysis of test data, field returns and existing modelling. It aims to enable a realistic assessment of electronic equipment reliability, including systems operating in severe environments (e.g. defence systems, aeronautics, industrial electronics, and transport).

The FIDES guide is divided in two parts : a reliability prediction guide and a reliability process control and audit guide. By identifying the factors contributing to reliability, whether technological, physical or process-based, FIDES allows the revision of product definition and intervention throughout the product lifecycle, to improve and control reliability. FIDES last revision is available at http://fides-reliability.org/.

9.2.3 HRD5

The British Telecom Handbook of reliability data, HRD5 is a reliability standard developed by British Telecommunications plc that also provides models for a wide range of components. In general, HRD5 is similar to CNET 93, but provides simpler models and requires fewer data parameters for analysis. The HRD5 method is available in a number of commercially available reliability software packages but the original handbook is no longer on sale

9.2.4 IEEE Gold Book

The IEEE Gold book IEEE recommended practice for the design of reliable, industrial and commercial power systems provides data concerning equipment reliability used in industrial and commercial power distribution systems. Reliability data for different types of equipment are provided along with other aspects of reliability analysis for power distribution systems, such as basic concepts of reliability analysis, probability methods, fundamentals of power system reliability evaluation, economic evaluation of reliability, and cost of power outage data.

More information about the IEEE Gold Book can be found on the IEEE website (http://www.ieee.org).

9.2.5 IRPH

IRPH ITALTEL Reliability Prediction Handbook is the Italian telecommunication companies version of CNET RDF. The standards are based on the same data sets with only some of the procedures and factors changed.

The Italtel IRPH handbook is available on request from:

Direzione Qualità, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy.

9.2.6 MIL-HDBK-217

MIL-HDBK-217, Reliability Prediction of Electronic Equipment, has been the mainstay of reliability predictions for about 40 years.

The handbook was published by the Department of Defense, Washington DC, U.S.A, and is available via several websites on the internet. Its last issue is the Rev. F + Notice 2.

The handbook is incorporated within several commercially available reliability software packages.

9.2.7 PRISM (RAC/ EPRD) now 217Plus

The RAC (EPRD) Electronic Parts Reliability Data Handbook database is the same as that previously used to support the MIL-HDBK-217, and is supported by a software tool marketed under the name of PRISM, which is also available as a module of several commercial reliability software packages. The models provided differ from those within MIL-HDBK-217.

The PRISM software is available from the address below, or is incorporated within several commercially available reliability software packages:

The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

9.2.8 RDF 2000 (UTE C 80-810, IEC-62380-TR Edition 1)

RDF 2000 is the latest version of the CNET handbook which was previously published as RDF93. This handbook has been adopted by UTEC and is known as the UTEC80810 Reliability Data Handbook. Recently this handbook has been adopted by IEC under the name IEC-62380-TR - Reliability Data Handbook – Universal model for reliability prediction of electronics components, PCBs and equipment.

This handbook covers most of the same components as MIL-HDBK-217. The models take into account power on/off cycling as well as temperature cycling and are very complex, with predictions for integrated circuits requiring information on equipment outside ambient and print circuit ambient temperatures, type of technology, number of transistors, year of manufacture, junction temperature, working time ratio, storage time ratio, thermal expansion characteristics, number of thermal cycles, thermal amplitude of variation, application of the device, as well as per transistor, technology related and package related base failure rates.

The standard IEC-62380 is available at:

The UTE UNION TECHNIQUE DE L'ÉLECTRICITÉ ET DE LA COMMUNICATION, Immeuble VOLTA, 33, avenue du Général Leclerc - BP 23, 92262 Fontenay-aux-Roses Cedex, France.

9.2.9 Siemens SN29500

The Siemens SN29500 Failure Rates of components and expected values method was developed by Siemens AG for use by Siemens and Siemens associates as a uniform basis for reliability prediction. The standard presented in the document is based on failure rates under specified conditions. The failure rates given were determined from application and testing experience taking external sources (e.g. MIL-HDBK-217) into consideration. Components are categorized into many different groups, each of which has a slightly different reliability model. The π factors used in this model take into account the variations in device operating temperature and electrical stress.

The standard is available on application to Siemens suppliers and customers of Siemens only and can be obtained through your contact person in the company.

9.2.10 Telcordia SR-322

The SR–332, Reliability Prediction Procedure for Electronic Equipment, completely replaces TR-332, Issue 6, and documents the recommended methods for predicting device and unit hardware reliability. The document contains several forms and tables to facilitate the derivation of reliability predictions. It contains instructions for suppliers to follow when providing predictions of their device, unit, or serial system reliability.

Device and unit failure rate predictions generated using this procedure are applicable for commercial electronic products whose physical design, manufacture, installation, and reliability assurance practices meet the appropriate Telcordia (or equivalent) generic and product-specific requirements.

The Telcordia SR–332 is available from the address below:

Telcordia Technologies, Inc., 8 Corporate Place, PYA 3A-184, Piscataway, NJ 08854-4156, U.S.A.

The Telcordia SR–332 is incorporated within several commercially available reliability software packages.

9.3 Mechanical Parts

9.3.1 NPRD

NPRD data provides failure rates for a wide variety of items, including mechanical and electro-mechanical parts and assemblies. The document provides detailed failure rate data on over 25000 parts for numerous part categories grouped by environment and quality level. Because the data does not include time-to-failure, the document is forced to report average failure rates to account for both defects and wear-out. Cumulatively, the database represents approximately 2,5 trillion part hours and 387000 failures accumulated from the early 1970's through 1994. The environments addressed include the same ones covered by MIL-HDBK-217; however, data is often very limited for some environments and specific part types. For these cases, it then becomes necessary to use the "rolled up" estimates provided, which make use of all data available for a broader class of parts and environments. Although the data book approach is generally thought to be less desirable, it remains an economical means of estimating "ballpark" reliability for mechanical components. This is available from the Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A

9.3.2 NSWC – Handbook of Reliability Prediction Procedures for Mechanical Equipment

This handbook, developed by the Naval Surface Warfare Center – Carderock Division, provides failure rate models for fundamental classes of mechanical components. Examples of the specific mechanical devices addressed by the document include belts, springs, bearings, seals, brakes, slider-crank mechanisms, and clutches. Failure rate models include factors that are known to impact the reliability of the components. For example, the most common failure modes for springs are fracture due to fatigue and excessive load stress relaxation. The reliability of a spring therefore depends on the material, design characteristics and the operating environment. NSWC models attempt to predict spring reliability based on these input characteristics. The drawback of the approach is that, like the physics of failure models for electronics, the models require a significant amount of detailed input data (e.g. material properties, and applied forces) that is often not readily available. They also do not address the issue of manufacturing defects. Data can also be collected from a wide range of applications and stress profiles, and is often grouped based on similar part types and application environments.

10. ANNEX B: LIST OF RELATED ON-GOING AND PLANNED ESA STUDIES WITH OBJECTIVES

10.1 Quantitative Reliability Requirements for Space Applications

The objectives of the quantitative reliability requirements for space applications study are the following:

- To identify when it is relevant or not in the scope of possible ESA programmes and missions to use and to specify quantitative reliability requirements (QR).
- To identify the most suited quantitative reliability parameters or attributes to be specified for a system, subsystem and unit.
- To establish a methodology to define QR requirements with respect to criteria to be identified (e.g. mission success criteria) and suitable means for their allocation and break down to lower levels (e.g. flight segment – ground segment, subsystem, equipment)
- To establish a methodology to define QRs with respect to criteria to be identified (e.g. mission success criteria).
- To identify the most suited quantitative reliability parameters or attributes to be specified for a system, subsystem and unit.
- To allocate them from system to subsystem, from subsystem to unit.

10.2 Reliability Data Sources and Methodologies for Space Applications

The primary objective of the study is to propose alternatives to the obsolete MIL-HDBK-217F (Notice 2) widely used today for reliability prediction in the European space community.

In particular, the study shall evaluate existing reliability prediction guidelines and study their suitability for application in the space domain.

The output of the study will be used to provide a common set of data as an input to update the ECSS handbook “Components reliability data sources and their use” ref. ECSS-Q-HB-30-08A.

10.3 New Reliability Prediction Methodology Aimed at Space Applications

The objective of the study is to develop a new reliability prediction methodology for space systems in an attempt to overcome the inherent limitations of the prediction practices which are currently based on outdated or limited handbooks that are still widely used by the space industry (e.g. MIL-HDBK-217).

Feedback from industry have highlighted the excellent reliability performances and fully satisfactory operational suitability of their systems and products often exceeding the lifetime expectations. However, there is a perception of over-design and consequently reduced cost effectiveness during the development process, especially when predictions are proven to be largely conservative with respect to the actual in-orbit performances.

The new reliability prediction methodology aims to improve the accuracy of the reliability predictions results and their effectiveness in supporting the analysis of alternative design solutions, as well as evaluating the conservativeness of design margins with respect to cost savings opportunities.

This study links to the TEC-QQD Safety & Dependability R&D Roadmap and the Reliability Assessment Roadmap harmonised with Industry [AWARE Workshops] with respect to the domain of “Methods, tools & data for reliability assessment”.

10.4 Reliability of Mechanical Systems and Parts

The objectives of this study are to:

- Define the most suitable methods to analyse and assess the reliability of mechanical systems and parts
- Provide methods and procedures for reliability verification by testing
- Provide inputs for the development of a handbook on reliability assessment of mechanical systems and parts (applicable to any future space mission)

10.5 RIDE: RAMS Exploitation of In-orbit Data

The objective of this study is to enhance the quality of RAMS analyses and risk assessments in future ESA programmes by feeding back findings from data collected during the operation of spacecraft in-orbit into the RAMS, risk assessment, and engineering (design and test) activities.

The initial activity investigated the possibility for implementing such evaluation and feedback capability by identifying the data to be collected, the availability of this data in ESOC’s various data repositories, and the preliminary definition of the user requirements to be met by such system.

A follow-up activity (RIDE demonstrator tool) based on the outcome of the initial study focuses on the four main objectives described below:

- Formulate and consolidate the concept and approach to exploit in-orbit data for dependability and risk-informed decision purposes during the design, verification, and operation of ESA spacecraft. Identify main stakeholders benefiting from this approach and the ways the interface.
- Assess the reusability of the existing ESA infrastructure (e.g. ARTS, SSYSSTER, MUST, MAT€D, etc.) and available tools (e.g. Dr. MUST) to provide the functionalities required to exploit in-orbit data, on one side, and to populate the “RIDE Utilisation System” on the other. Identify complementary technology for

missing functionalities (e.g. text mining). Define the tools necessary to access, aggregate and visualise the information (e.g. web services for desktop visualisation).

- Define the processes and the interfaces to existing systems/tools required for enabling the access, the aggregation, and the dissemination of information coming from design, verification, and operations across different directorates or programme boundaries such that any user within ESA can benefit from this data pool for dependability and risk assessments using in-orbit data.
- Validate the suitability of the approach to exploit RAMS related in-orbit data through a proof of concept demonstrator to be used by design, verification, and operation teams across different missions/programmes.