

# New statistical formulations for determination of qualification test plans of safety instrumented systems (SIS) subject to low/high operational demands

Y. F. Khalil, Ph.D., Sc.D.

*Yale University & United Technologies Research Center (UTRC), USA*

## Abstract

This paper aims to develop new statistical formulations to design efficient reliability demonstration test (RDT) plans for electrical/electronic and programmable electronic (E/E/ES) safety instrumented systems (SIS) subject to requirements of IEC 61508-1 (2010) standard.<sup>1</sup> A case study is presented to show how the proposed statistical formulations can be employed to design RDT plans to validate whether SIS target mission reliability (TMR) can be met under a specified confidence level. Discussions includes trade-offs between test duration and number of units on test and sensitivity studies showing how the demonstrated reliability at end of mission life is impacted by SIS operational mode and key statistical parameters. The major contributions that this research offers are: i) A framework to guide reliability practitioners in applying the proposed statistical formulations to design optimum RDT plans and articulate mission reliability statements (MRS) to support regulatory certification of new SIS designs. ii) A methodology, demonstrated by a practical case study, to show how RDT plans can be designed to meet targets set by the applicable standards. The developed framework is robust and can support certification of safety systems in a wide variety of industrial applications.

**Keywords:** Mission reliability; design life; safety instrumented system; mission statement; mission life; reliability demonstration

---

## Abbreviations

ALRDT	Accelerated life reliability demonstration test
$C_{TML}$	Coefficient ( $\geq 1$ ) signifying multiples of SIS target mission life (TML) - Eq. (9)
$C_{TML,HD}$	Coefficient of TML under high-demand mode of operation. It signifies multiples of TML - Eq. (11)
$C_{TML,LD}$	Coefficient of TML under low-demand mode of operation. It signifies multiples of TML - Eq. (10)

---

<sup>1</sup> IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic (E/E/ES) safety-related systems. Source: <http://www.iec.ch/functionalsafety/standards/>

$CL$	Confidence level = $1 - \alpha$ ; where $\alpha$ is Type-II statistical error ( <i>aka</i> , the consumer's risk).
$DML$	Demonstrated mission life
$PFD_{avg}$	Average failure probability on demand (refer to Table 1)
PFH	Average failure probability per hour (refer to Table 1)
MRS	Mission reliability statement
$N$	Number of test units in Eq. (3) that need to be tested failure free during the specified test duration (either in cycles or hours)
$N'$	Number of test units in Eq. (5) that need to be tested failure free during the specified test duration (either in cycles or hours)
RDT	Reliability demonstration test. It is a stress test that aims to determine whether the product can meet a specified reliability goal at end of design life
$R_{TML}$	Reliability of SIS at time equals to the target mission life ( <i>aka</i> . design life)
SIL	Safety integrity levels defined in IEC 61508-1(2010)
SIS	Safety instrumented system
$t_{TML}$	Time equal to target mission life ( <i>aka</i> . design life)
TML	Target mission life ( <i>aka</i> . design life)
TMR	Target mission reliability

Note: In this paper, the terms ALRDT and RDT are used interchangeably. Also, the terms design life and target mission life (TML) are used interchangeably.

## 1. Introduction

This section is divided into three subsections that begin with a brief background of previous relevant publications and description of the functional safety standard IEC 61508-1 [26] in subsection 1.1. A description of objectives of this study is provided in subsection 1.2. Finally, a statement highlighting importance and novelty of this work is presented in subsection 1.3.

### 1.1 Background

#### 1.1.1 Literature review

Reliability demonstration under a specified level of statistical confidence is a prerequisite for the regulatory certification process of newly-designed safety instrumented systems (SIS). Accordingly, reliability practitioners are typically tasked with determination of how many units are to be tested (either without failures or with one or more allowed failures as test decision criterion), for how long, and under what conditions in order to demonstrate a target mission reliability (TMR) at the end of a specified design life with a specified confidence level (CL). The rationale for linking system reliability to some level of statistical confidence stems from the fact that reliability practitioners attempt to formulate mission reliability statements based on small samples of test units. Identification of an efficient RDT decision rule/criterion (*viz.*, allowed number of failed units during testing) is yet another expectation to be addressed by reliability practitioners.

Our literature review identified several research efforts that discuss the optimum designs of RDT plans under different conditions [1-25, 32-35]. One of the commonly cited RDT plans is the conventional bogey test (CBT) method which tests a sample of units at the use stress level for a specified test duration. For CBT, the required reliability is demonstrated if no failures occur during the testing [1]. As noted by the author, CBT demonstrates only the lower-bound reliability (*viz.*, failure point) rather than monitoring and measuring degradation of the test units during the conduct of the test [1]. Accordingly, he proposed use of non-destructive methods to periodically test each one of the units to measure potential degradation and calculate the conditional failure probability of each unit on test. The test can be terminated earlier if the degradation level in any of the units on tests exceeds an acceptable threshold [1]. Our literature review also revealed that published work related to RDT plans varied depending on the censoring scheme (*viz.*, time censoring vs. failure censoring), assumed service life time distribution (*e.g.*, exponential, Weibull, lognormal, logistic, etc.), and testing conditions. Methods to determine the optimum sample size and the test duration for an RDT / ALRDT have been studied extensively. In general, these methods can be classified as: a) test designs based on the number of allowed failures [4,5,8] and b) test designs based on failure times [4]-[7].

This subsection provides highlights of selected published work over the past two decades as follows: McKane, Escobar, and Meeker, 2005 [8] reviewed available statistical methods of demonstration tests involving the failure-censored scheme in which RDT is conducted until a specified number of failures occurs. Feyzioglu et al., 2006 [9] argued that conducting individual component tests for prediction and verification of system reliability is more advantageous compared to system-level testing, as the latter could be economically unfeasible or even impossible. Accordingly, they proposed an optimal component-level RDT plan using a semi-infinite linear program. Idris and Aladin, 2013 [10] proposed RDT plans using a structured design for six sigma method, *viz.*, Define, Measure, Analyze, Design and Verify (DMADV). The DMADV steps cover the process from early stage until the end stage of developing the RDT plan. Their proposed RTD plan considered processes of the product design life cycle including market or customer needs, reliability requirements, cumulative effects of use environment, design life probability distribution and tests of equipment capabilities. Luo et al., 2015 [11] developed a time-censored accelerated degradation testing (ADT) methodology based on reliability target allocations under competing failure modes at accelerated conditions. The reliability target of the system was first allocated to each failure mode, and according to those allocations, the plan for each failure mode under the accelerated condition was designed. The authors claim that the degradation measurements can be used to predict whether the test unit would fail at the censoring time and, henceforth, the test duration could be reduced. In our opinion, accuracy of the proposed claim is highly uncertain due to the difficulty of observing the exact points in time where failures or degradation mechanisms change from one type to another. Moreover, if sufficient test time is not provided to identify such change points, reliability predictions could be biased as a result of missing key failure modes. Lu et al., 2016 [12] explored the interrelationship between multiple objectives when planning a demonstration test and proposed structured decision-making procedures using a Pareto approach for selecting an optimal test plan based on simultaneously balancing multiple criteria. Li, P. et al., 2017 [13] proposed an accelerated approach for determining system-level reliability target of each environmental stressor (*e.g.*, thermal cycling, thermal dwell, vibration, humidity level, etc.) and for competing failure modes. While we support the conduct of a separate accelerated test for each environmental stressor, our doubts remain about

the accuracy of the accelerated tests that are designed to identify multi failure modes. Most recently, Kumar and Bajeel, 2018 [14] proposed an optimal RDT plan based on a maximum likelihood estimator (MLE) of system reliability using exponential probability distributions subject to risk factors, which they called the covariates (*viz.*, temperature, pressure, etc.). The covariates were assumed to affect the reliability of the system. They concluded that the optimum RDT design depends upon cost of the individual component and number of components in the system. In our opinion, the mathematical treatment approach of the environmental stressors as covariates failed to account for the interaction terms among the covariates (*e.g.*, temperature\*pressure interaction term and so on). Since this manuscript is not intended to be a review paper of relevant literature, interested readers who would like to know more about merits and limitations of the previously proposed RDT and ADT plans can read the review papers by Yang [32], Elseyed [33], Escobar and Meeker [34], and Luo et al. [35].

We conclude this literature review subsection by stating that reliability practitioners as well as other stakeholders always seek RDT plans that minimize testing duration to reduce associated costs and lead times before a new system design can be certified by the relevant regulatory bodies and released for field deployment [25].

### 1.1.2 IEC 61508-1:2010 Standard

The functional safety standard IEC 61508-1 [26] follows a risk-based approach to establish requirements for electrical /electronic/ programmable electronic (E/E/PES) systems. A system is assumed to be safety-related if its failure to function can lead to human harm.

The Safety integrity level (SIL) rating defines the average probability that the safety related system could fail in a dangerous mode of failure. As Table 1 (*adapted from IEC 61508-1*) shows, the value of SIL rating ranges from 1 (which is the lowest rating) to 4 (which is the highest SIL rating). Also, SIL ratings and ranges are defined for two modes of operation, *viz.*, a low-demand mode and a high-demand mode.

**Table 1**

Ratings of safety integrity levels (SIL) per IEC 61508-1:2010 [26].

Safety Integrity Level (SIL)	Low-Demand Mode of Operation ( $PFD_{avg}$ )	High-Demand or Continuous Model of Operation (PFH)
4 (highest rating)	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1 (lowest rating)	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

$PFD_{avg}$  = average failure probability on demand

$PFH$  = average failure probability per hour

Notes:

- a) All failures shown in Table 1 are dangerous failures (*both detected and undetected*).
- b) The information summarized in Table 1 is cited in Tables 2 and 3 of IEC 61508-1 [26] as well as in Tables 3 and 4 of IEC 61511-1 [27].

*Interpretation example of SIL ratings (as defined in Table 1)* - For low-demand mode of operation, a SIL 2 system (or component) means that the maximum acceptable  $PFD_{avg}$  (*viz.*, upper bound) is one dangerous failure (whether detected or undetected) in 100 years. Similarly, a SIL 3 system (or component) signifies that the maximum acceptable  $PFD_{avg}$  (*viz.*, upper bound) is one dangerous failure per 1000 years.

It is important to note that if there is a gap between the calculated SIL rating and the target SIL rating, then risk reduction methods should be pursued and, accordingly, the ALARA principle ‘As low as reasonably achievable,’ should apply by adding additional layers of protection (LOP). In this regard, a cost-to-benefit analysis (CBA) would be required to ensure that the proposed LOPs are achievable and practicable.

## 1.2 Objectives

The primary objectives of this paper are four-fold as follows:

- a) Propose new statistical formulations that can be used by reliability practitioners to design efficient RDT plans of safety instrumented systems (SIS) subject to IEC 61508-1 (2010) standard [26]. The RDT plans can be used to demonstrate whether a new SIS design can achieve TMR at the end of the desired design life with a specified  $CL$ . Herein, the primary focus is on zero-failures allowed RDT<sup>2</sup> decision criterion to provide the minimum sample size plan.
- b) Construct an at-a-glance framework that describes the steps of designing the RDT plan.
- c) Formulate SIS mission reliability statement (MRS) under the assumed mode of operation (low vs. high demands) and specified  $CL$ .
- d) Provide a practical case study with associated numerical examples to show the impact on RDT plan of key statistical parameters (*e.g.*,  $CL$  and Weibull shape parameter,  $\beta$ ), number of allowed failures during testing, and SIS operational modes (*viz.*, low- and high-demand).

## 1.3 Importance and novelty of this work

This work is motivated by the fact that execution of inefficient RDT plans can be time-consuming, labor intensive, and costly. Additionally, to this author’s best knowledge, none of the published work has addressed the niche area of reliability demonstration required to support regulatory certification of new SIS designs. Hence, the novelty of this contribution is manifested

---

<sup>2</sup> While the zero-failure RDT is intended to reduce the consumer’s risk, it also leads to increasing the producer’s risk of rejecting a sufficiently reliable product design.

by its goal of filling the current void in state of knowledge about reliability demonstration of new SIS designs.

The methodology and insights provided herein can assist reliability practitioners to: i) Design efficient RDT plans to predict, with some level of statistical confidence, whether the stated TMR can be met at end of SIS design life and ii) Formulate MRS that can be used to support the regulatory certification process of new SIS designs.<sup>3</sup>

The remaining sections of this manuscript are organized as follows: Section 2 describes the proposed statistical framework. Section 3 presents the results of applying the proposed statistical formulations to a case study with its associated numerical examples to illustrate how the proposed framework can be applied to design optimum RDT plans and formulate informative MRS. Discussion of key insights derived from the generated results is also covered in Section 3. Finally, Section 4 concludes with brief highlights of major insights to support reliability practitioners' efforts to obtain regulatory certification of new SIS designs. The insights of this work can also be used to support efforts to obtain relief from highly conservative regulatory requests that may cause undue burdens (time and cost) on manufacturers of new products. An example of undue regulatory burdens could be a request for using 99% *CL* in reliability predictions while 90% *CL* could be more appropriate for the intended application. The key insights of this work could also be used for justifying specific assumptions such as assuming a Weibull shape parameter ( $\beta$ ) of 3.5 in lieu of a lower value, say  $\beta = 2$ .

## **2. Statistical methods for designing RDT plans**

This section is divided into the following six subsections: Subsection 2.1 which presents the non-parametric binomial method [12] for determination of the minimum number of units on test. Subsection 2.2 introduces the proposed statistical formulations that extend applicability of the parametric binomial Lipson equality [2] to safety instrumented systems (SIS) subject to IEC 61508-1:2010 [26] requirements for low- and high-demand modes of operations. Subsection 2.3 provides at-a-glance framework of the proposed statistical approach to guide reliability practitioners in designing efficient RDT plans and developing associated MRS. Subsection 2.4 highlights the benefits of selecting zero-failures allowed as the RDT decision criterion. Section 2.5 presents key features of Weibull shape parameter ( $\beta$ ) and finally subsection 2.6 discusses the formulation of SIS mission reliability statement.

### ***2.1 The nonparametric binomial test method***

Use of the nonparametric binomial method [12] to design an RDT plan based on the number of allowed failures ( $K$ ) of the units on test is straightforward as described by Eqs. (1) through (3).

---

<sup>3</sup> The author of this manuscript taught graduate courses on risk assessment and reliability engineering at Yale University and the Massachusetts Institute of Technology. He also was the Engineering Manager of the Probabilistic Risk Assessment (PRA) Department at the Millstone Nuclear Power Station in Connecticut, USA and has contributed to risk-informed and reliability-based regulatory certification of safety systems in the nuclear and chemical industries.

$$CL = 1 - \sum_{i=0}^{K} \frac{N!}{i!(N-i)!} \cdot (1-R)^i \cdot R^{N-i} \quad (1)$$

Where:

$CL$  = a user-specified confidence level (%). The value of this statistical parameter is industry-specific as well as product-dependent and may range from 70% up to  $\geq 99\%$ . In general, however, an 80%  $CL$  is considered to be acceptable [23].

$R$  = SIS target mission reliability (%). This is the reliability (*viz.*, probability of success) level to be demonstrated.

$K$  = number of allowed failures of units on test, where  $i = 0, 1, 2, \dots K$ . The number of failed units during RDT performance reflects the demonstrated reliability with a specified  $CL$ .

$N$  = number of units on test (*viz.*, sample size). Besides its dependence on the specified  $CL$  and test duration. Other factors that may impact the selected value of  $N$  include availability of pilot units for testing, laboratory's physical constraints (*viz.*, size of the environmental chamber available for testing), resources available to monitor the units during testing, cost of conducting the tests, and schedule for release of field units.

For a zero-failures allowed as RDT decision criterion,  $K = 0$ , and, hence, Eq. (1) reduces to:

$$CL = 1 - R^N \quad (2)$$

Eq. (2) is called the '*success run formula*,' as 100% success rate of the units on test is required. This equation can be solved for the number of units on test  $N$  as follows:

$$N = \frac{\ln(1-CL)}{\ln(R)} \quad (3)$$

In Eq. (3) and for a given  $CL$ , as target mission reliability  $R$  approaches 100%, the required number of units on test  $N$  approaches infinity. Also, the term  $(1-CL)$  in the numerator of Eq. (3) represents Type-II statistical error (*viz.*, consumer's risk).

## 2.2 Proposed statistical formulations

The new statistical formulations discussed in this subsection extend the parametric binomial Lipson equality [2] to SIS applications subject to IEC 61508-1:2010 standard [26]. Therein, a system is assumed to be safety-related if its failure to function under a stated mode of operation can lead to human harm. According to IEC 61508-1:2010 [26] standard, SIS can be assigned a safety integrity level (SIL) rating that defines the average probability that the safety-related system could fail in a dangerous mode (whether it is dangerous detected or dangerous undetected failure mode).

In the parametric binomial approach, it is assumed that the system's mission life can be described by a 2-paramter ( $\beta, \eta$ ) Weibull distribution. The shape parameter ( $\beta$ ) can be assumed based on

prior technical knowledge of the reliability practitioner about  $\beta$  values of other surrogate / proxy systems or field failure data. Alternatively, the  $\beta$  value can be calculated by fitting a 2p-Weibull model using accelerated life RDT (ALRDT) data. When the zero-failures allowed decision criterion is selected, the associated RDT is required to continue until at least one of the test units fails before completing the required number of test cycles. The number of test cycles of the first test unit to fail poses a limit on the demonstrated reliability even other test units could fail at higher numbers of test cycles (Refer to subsection 3.8 for more details). The ALRDT is typically performed under a specified external stressor. Examples of the external stressors may include high humidity level, temperature cycling, thermal dwell, mechanical vibration (random or harmonic), on/off power cycling, thermal (or mechanical) shock, over-voltage, etc.

The equation that represents the zero-failures allowed decision criterion can be described by Eq. (4) as follows:

$$R = (1 - CL)^{\frac{1}{N' \cdot C_{TML}^\beta}} \quad (4)$$

Where  $C_{TML}$  is a coefficient (typically has a value  $\geq 1$ )<sup>4</sup> signifying multiples of TML. For example,  $C_{TML}$  of 4 means RDT duration is four times TML (expressed in cycles or hours). Again,  $\beta$  in Eq. (4) is the 2p-Weibull shape parameter,  $N'$  is the number of units on tests, and the demonstrated reliability at TML, viz.,  $R = R_{TML}$ .

Eq. (4) can be rearranged as shown by Eq. (5) to be able to calculate the number of units  $N'$  on test:

$$N' = \frac{\ln(1-CL)}{C_{TML}^\beta \ln(R)} \quad (5)$$

Note that Eqs. (3) and (5) are similar except that Eq. (3) is independent of the shape parameter  $\beta$  and in Eq. (5), the calculated number of units on test  $N'$  is lesser than  $N$  calculated via Eq. (3) as the right-hand-side of Eq. (3), viz.,  $\frac{\ln(1-CL)}{\ln(R)}$ , is now divided by  $C_{TML}^\beta$ . For example, if  $C_{TML} = 4$  and  $\beta = 3$ , then  $C_{TML}^\beta = 4^3 = 64$ . Henceforth, the number of units of test ( $N'$ ) calculated by Eq. (5) is 64 times less than the number of units on test  $N$  as calculated by Eq. (3). If  $\beta = 2$  instead of 3, then  $C_{TML}^\beta = 4^2 = 16$  and, henceforth,  $N' = \frac{N}{16}$  in lieu of  $\frac{N}{64}$  when  $\beta = 3$ . That is say, as  $\beta$  value increases from 2 to 3, the number of test units decreases by 25%. Table 2 and Fig. 5 in subsection 3.2 show how RDT duration varies with Weibull shape parameter ( $\beta$ ) and the number of units on test ( $N'$ ).

---

<sup>4</sup> It is possible that the value of  $C_{TML}$  could be  $< 1$ . In such case, the number of units on test would increase, given any assumed value of  $\beta$  greater than its true value.



Eq. (5) can be manipulated to calculate  $C_{TML}$  as follows:

$$C_{TML}^{\beta} = \frac{Ln(1-CL)}{N'.Ln(R(t))} \quad (6)$$

Taking the natural logarithm of both sides of Eq. (6) yields Eq. (7) as follows:

$$\beta.Ln(C_{TML}) = Ln \left\{ \frac{Ln(1-CL)}{N'.Ln(R(t))} \right\} \quad (7)$$

Eq. (7) can be further rearranged as shown by Eq. (8) to allow the calculation of  $C_{TML}$ .

$$C_{TML} = EXP \left\{ \frac{1}{\beta} . Ln \left[ \frac{Ln(1-CL)}{N'.Ln(R(t))} \right] \right\} \quad (8)$$

At end of SIS target mission life,  $t = t_{TML}$ ,  $R(t) = R_{TML}$ , hence:

$$C_{TML} = EXP \left\{ \frac{1}{\beta} . Ln \left[ \frac{Ln(1-CL)}{N'.Ln(R_{TML})} \right] \right\} \quad (9)$$

### 2.2.1 Safety Instrumented System subject to low-demand (LD) mode of operation

For *LD* mode of operation, IEC 61508-1 provides lower and upper bounds for the average failure probability on demand,  $PFD_{avg}$ , for each SIL rating as summarized in Table 1. Accordingly, Eq. (10) for *LD* mode of operation can be expressed as follows:

$$C_{TML,LD} = EXP \left\{ \frac{1}{\beta} . Ln \left[ \frac{Ln(1-CL)}{N'.Ln(1-FPD_{avg})} \right] \right\} \quad (10)$$

In Eq. (10),  $C_{TML,LD}$  is the coefficient of TML under *LD* mode of operation. It signifies multiples of *TML*.

Finally, the required number failure-free test cycles =  $TML$  (in cycles) \*  $C_{TML,LD}$

### 2.2.2 Safety Instrumented System subject to high-demand (HD) mode of operation

For *HD* mode of operation, IEC 61508-1 provides lower and upper bounds for the average failure probability per hour,  $PFD_{avg}$ , for each SIL rating as summarized in Table 1. Accordingly, Eq. (11) for *HD* mode of operation can be expressed as follows:

$$C_{TML,HD} = EXP \left\{ \frac{1}{\beta} \cdot Ln \left[ \frac{Ln(1-CL)}{N' \cdot Ln(1-8760 \cdot FPH_{avg})} \right] \right\} \quad (11)$$

$C_{TML,HD}$  is the coefficient of TML under *HD* mode of operation. It signifies multiples of  $TML$ .

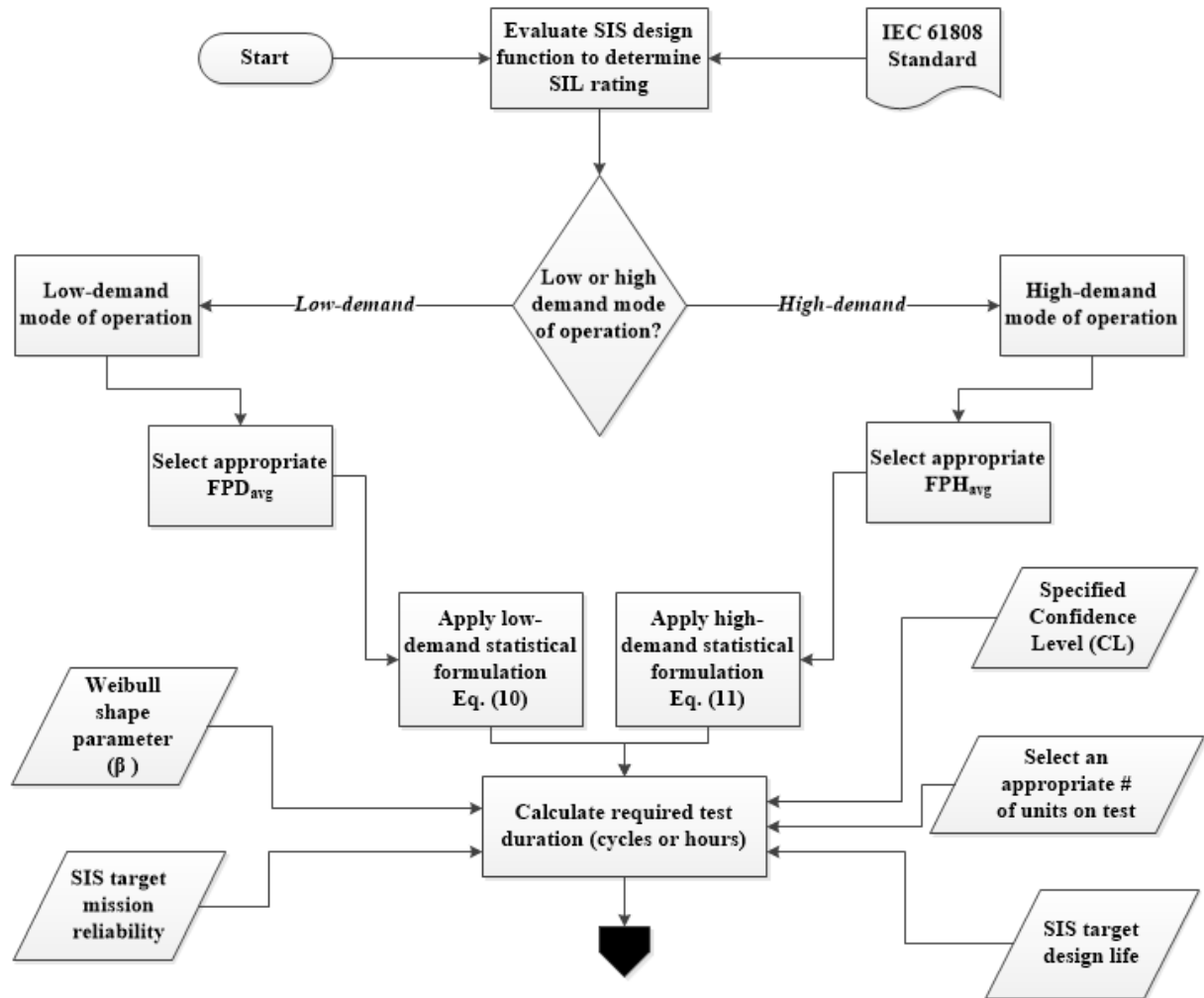
For *HD* mode of operation, the required number of failure-free test cycles =  $TML$  (in cycles) \*  $C_{TML,HD}$

### 2.3 At-a-glance roadmap for development of SIS reliability demonstration test plan

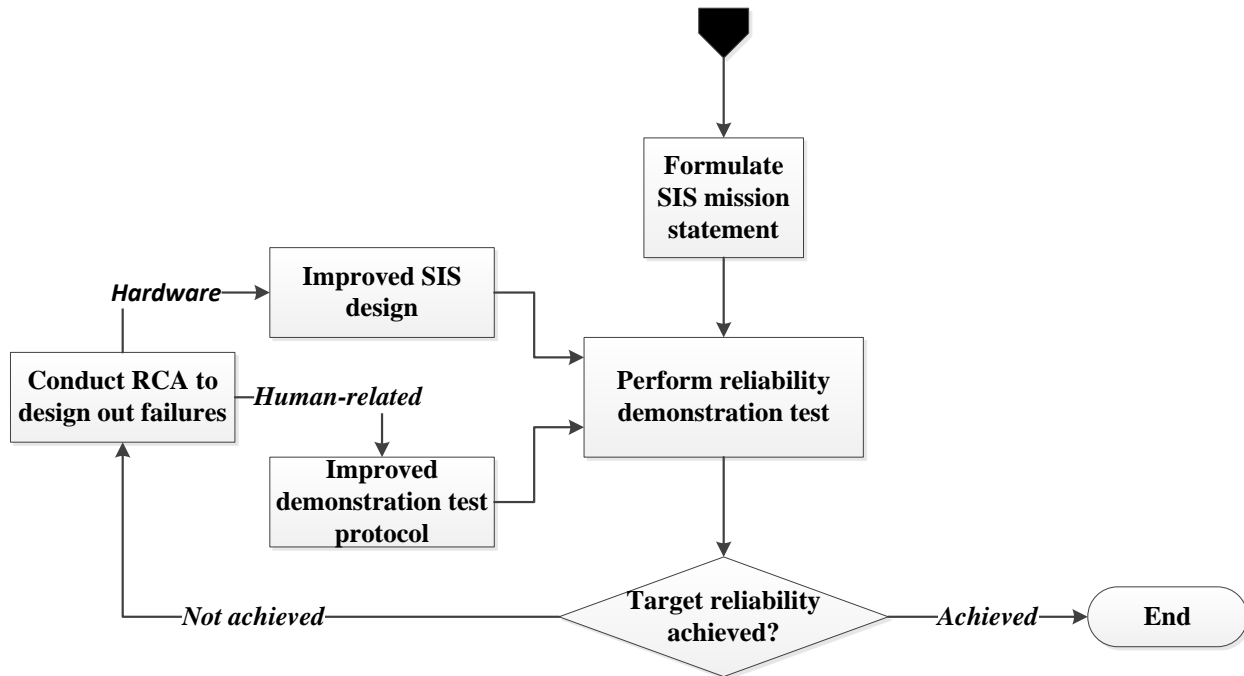
Figs. 1A and 1B provide a roadmap for designing SIS reliability demonstration test plan and formulating the mission reliability statement. Eqs. (10) and (11) for *LD* and *HD* modes of operations, respectively, can be employed to design the RDT plan for the reliability demonstration. Given that RDT plan is based on the zero-failures allowed decision criterion, there are four unknown parameters in these two equations, viz., the number of units on test  $N'$ ; average failure probability on demand (or average failure probability per hour); Weibull shape parameter  $\beta$ ; and  $CL$ . By assigning values for these four parameters, the required number of failure-free test cycles can be determined.

Value of the parameter  $\beta$  can be either assumed based on prior technical knowledge of the reliability practitioner or estimated from RDT data. More discussion on the impact of the value of  $\beta$  on the calculated test cycles is provided in subsection 3.2.

Fig. 1B shows that when the product target reliability is not achieved, root cause analysis (RCA) should be pursued to design out the identified failure modes. The scope of RCA also includes recommendations for additional experimental work to better understand newly identified failure mechanisms and their causes.



**Fig. 1A.** At-a-glance roadmap for development of SIS reliability demonstration test plan.



**Fig. 1B.** At-a-glance roadmap for development of SIS reliability demonstration test plan (cont'd).

## 2.4 Benefits of zero-failures allowed reliability demonstration tests

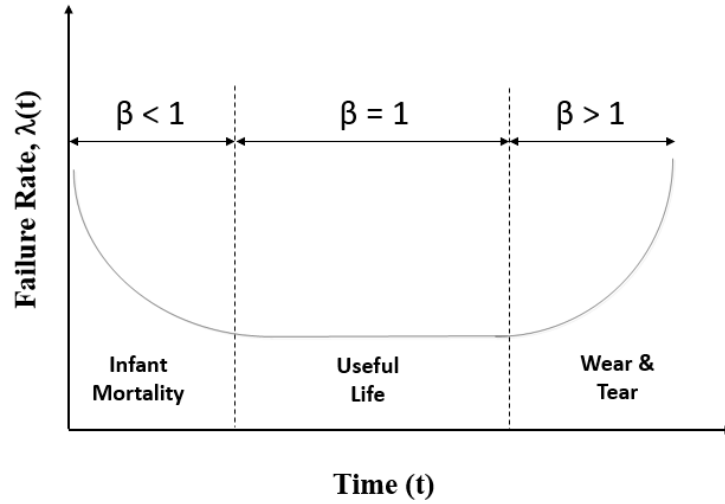
The zero-failures allowed RDT means that the test is successful if none of the tested units fail during the test. However, an unsuccessful RDT still offers key benefits. For example, conducting root cause analysis (RCA) on the failed units can uncover opportunities for component and system design improvements by designing out the root cause (or causes) of the identified failure mode (or modes). In addition to identifying hardware failures, RCA may also lead to identifying specific human-related or test protocol related errors. As the case may be, there are benefits and lessons to be learned from conducting RCA for failed test units.

While this subsection focused on highlighting the benefits of zero-failures allowed RDT plans, reliability practitioners should also be aware of one key limitation of this testing approach as follows: There could be a latent failure mode that does not manifest itself during the zero-failures RDT which uses the minimum sample size (i.e., number of units on test). This latent failure mode could show up when a larger population of units is fielded.

## 2.5 Weibull shape parameter $\beta$

Fig.2 shows a typical product lifecycle with the y-axis representing the failure rate,  $\lambda(t)$  and x-axis representing the time. As shown, the curve has three distinct regions. In the first region (left), the device failure rate,  $\lambda(t)$  is a decreasing function of time ( $t$ ). This region is called the infant (or early) mortality region and the value of Weibull shape parameter  $\beta$  is less than 1.0. The middle

region is called the useful life and failure could occur randomly with a constant failure rate. For the middle region, the Weibull shape parameter  $\beta$  equals 1.0. In the third region (right), device failure occurs due to wear and tear and Weibull shape parameter ( $\beta$ ) is greater than 1.0.



**Fig. 2.** ‘Bath-Tub Curve’ describing variability of the failure rate,  $\lambda(t)$ , as a function of time [29-31].

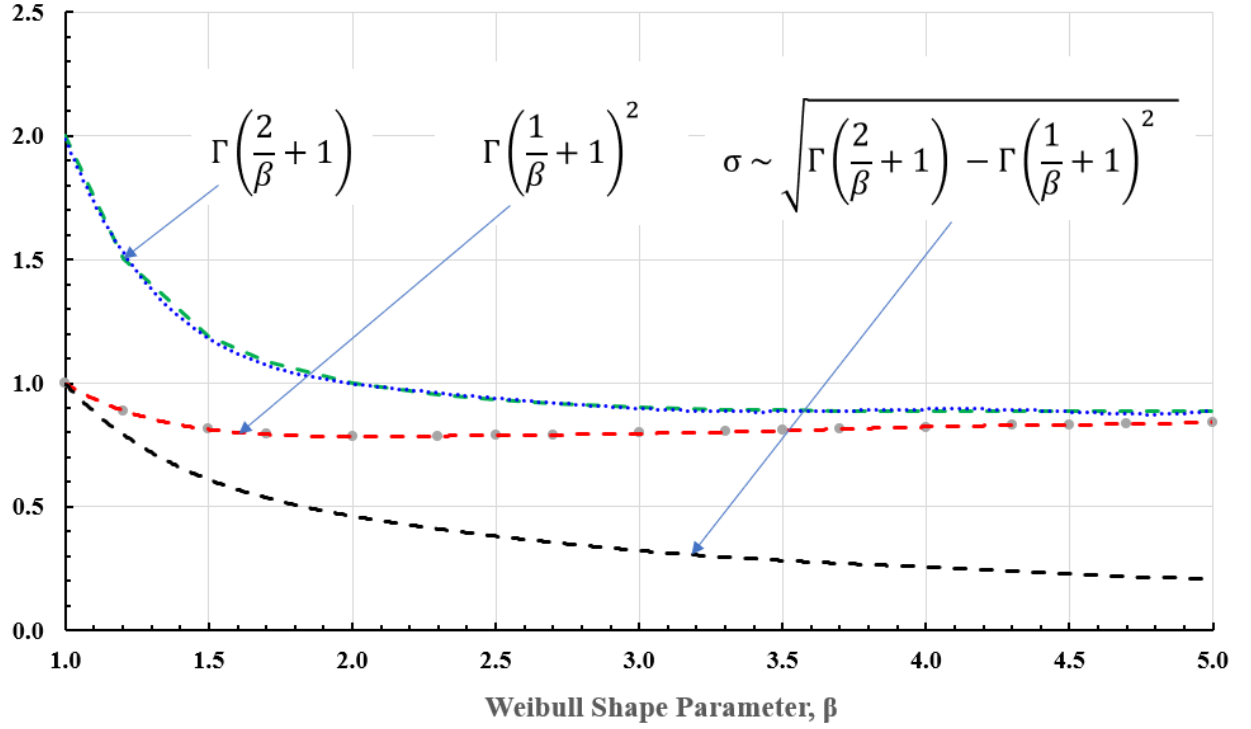
More discussion on the impact of  $\beta$  on the RDT plan is provided in subsection 3.2. However, it is worth mentioning the following couple of key insights about the role that the value  $\beta$  plays in designing RDT plans.

- For a given RDT duration, use of a  $\beta$  value smaller than it should be (say 2 compared to 3) would increase in the number of units on test.
- For a give Weibull characteristic life<sup>5</sup> ( $\eta$ ), the  $\beta$  parameter directly impacts the standard deviation ( $\sigma$ ) of the 2-parameter Weibull probability distribution as shown by Eq. (12).

$$\sigma = \eta \cdot \sqrt{\Gamma\left(\frac{2}{\beta} + 1\right) - \Gamma\left(\frac{1}{\beta} + 1\right)^2} \quad (12)$$

In Eq. (12),  $\Gamma\left(\frac{2}{\beta} + 1\right)$  and  $\Gamma\left(\frac{1}{\beta} + 1\right)$  are Gamma functions evaluated at  $\left(\frac{2}{\beta} + 1\right)$  and  $\left(\frac{1}{\beta} + 1\right)$ , respectively.

<sup>5</sup> Aka. Weibull’s scale parameter.



**Fig. 3.** Impact of the value of  $\beta$  on Weibull standard deviation,  $\sigma$ , Eq. (12).

The y-axis in Fig. 3 represents values of:

$\Gamma\left(\frac{2}{\beta} + 1\right)$ ,  $\Gamma\left(\frac{1}{\beta} + 1\right)^2$ , and  $\sqrt{\Gamma\left(\frac{2}{\beta} + 1\right) - \Gamma\left(\frac{1}{\beta} + 1\right)^2}$  for a range of  $\beta$  values from 1.0 to 5.0 (with an increment of 0.5).

As Fig. 3 shows,  $\Gamma\left(\frac{2}{\beta} + 1\right)$  which is the first term under the square root on right hand side in Eq. (12) decreases fast as the value of  $\beta$  increases from 1.0 to around 3.0 after which the impact of on the value of the first term diminishes. Similarly, as  $\beta$  increases the value of  $\Gamma\left(\frac{1}{\beta} + 1\right)^2$  which is the second term under the square root in Eq. (12) decreases up to  $\beta$  of  $\approx 2.3$  but then slightly increases as the value of  $\beta$  increases. Finally, the value of Weibull standard deviation,  $\sigma$ , which is proportional to  $\frac{1}{\beta}$ , decreases as  $\beta$  increases. Accordingly, the relationship between  $\sigma$  and  $\beta$  can be approximated as described by Eq. (13).

$$\sigma \approx \frac{1}{\beta} \quad (13)$$

In Eq. (13) which mathematically describes the dependence of  $\sigma$  on  $\beta$ , the inverse of this shape parameter, viz.,  $\frac{1}{\beta}$ , reflects the standard deviation ( $\sigma$ ), or spread of failure data points on a Weibull probability plot. Accordingly, as the value of  $\beta$  increases, the inverse value  $\frac{1}{\beta}$  would decrease and, henceforth, the standard deviation ( $\sigma$ ) or spread of failure data points would also decrease. For example,  $\beta = 3$  is more preferable (if the higher value is justifiable for SIS being tested) compared to  $\beta = 2$  because  $1/3$  is smaller than  $1/2$ . In summary, the parameter  $\frac{1}{\beta}$  not only describes the behavior of the failure rate  $\lambda(t)$  as a function of time, but also reflects the spread/ variability of test data points.

## **2.6 Formulation of SIS mission reliability statement**

A mission reliability statement provides a succinct and informative description of the operational conditions under which the stated target mission reliability of the system can be achieved at the end of specified design life with a specified level of statistical confidence. An example of system MRS at 90% CL can be articulated as follows:

*If N units are cycled for a required number of test cycles and none of units failed during testing before meeting the required number of cycles, then, with 90% confidence level, the target mission reliability can be achieved at the end of the specified design life under the stated operational conditions.*

More discussion on formulating product reliability mission statements (RMS) is provided in subsection 3.7

## **3. Results and discussion**

This section is divided into eight subsections as follows: Subsection 3.1 describes the case study and its assumptions. Subsection 3.2 discusses the impact of  $\beta$  on RDT plan. Subsection 3.3 highlights the impact of  $CL$  on RDT plan and subsection 3.4 compares the impact on RDT duration of low- and high-demand modes of operation. Subsection 3.6 highlights the impact number of failures allowed in RDT plans and subsection 3.7 provides examples of SIS mission reliability statements. Finally, subsection 3.8 shows how demonstrated mission life (DML) could differ from target mission life (TML).

### **3.1 Description of the case study**

To demonstrate the utility of the proposed statistical framework to design an efficient RDT plan, a practical case study has been formulated with the following assumptions:

- A safety instrumented system (SIS) with 15 years target design life (or equivalently 5,475 cycles, based on 365 cycles per year).
- TMR = 99.50% at end of the design life.

- Ten test units are available for RDT.
- Unless otherwise stated, all reliability calculations are to be conducted with 95%  $CL$ .

The case study together with its associated five numerical examples are designed to show how RDT duration and number of units on test ( $N'$ ) are impacted by the assumed statistical parameters ( $\beta$  and  $CL$ ), number of allowed failures during testing, and system's mode of operational (*viz.*,  $LD$  vs.  $HD$ ).

### 3.2 Impact of Weibull shape parameter $\beta$ on RDT plan

For RDT with  $C_{TML,LD} > 1$  (refer to Eq. (10) which defines  $C_{TML,LD}$ ), assuming a value of  $\beta$  less than its true value<sup>6</sup> would lead to a valid (although conservative) RDT plan with more than the necessary number of units on test (*i.e.*, overestimated number of test units). If, however, the assumed value of  $\beta$  is greater than its true value, then RDT plan is considered to be less conservative and possibly invalid since the number of units on test would be underestimated. The aforementioned statement related to  $C_{TML,LD}$  and  $\beta$  also applies to the case where  $C_{TML,HD} > 1$  (refer to Eq. (11) which defines  $C_{TML,HD}$ ).

Table 2 shows the impact of a range of values of  $\beta$  (from 0.5 to 4.0) on the required number of test units ( $N'$ ) for arbitrarily selected  $C_{TML}$  values of 2 and 4. The remaining parameters in Eq. (5), *viz.*, TMR and  $CL$  are provided in the description of the case study (Subsection 3.1).

**Table 2**

Impact of value of  $\beta$  on the required number of units on test,  $N'$  (refer to Eq. (5)).

Weibull Shape Parameter $\beta$	Calculated Number of Units on Test, $N'$ (Eq. 5)	
	$C_{TML} = 2$	$C_{TML} = 4$
0.5	423	299
1.0	299	149
1.5	211	75
2.0	149	37
2.5	106	19
3.0	75	9
3.5	53	5
4.0	37	2

*Notes:*

- The calculations shown in Table 2 are based on 95%  $CL$  and 99.50% TMR.
- $C_{TML} = 2$  signifies RDT duration equal to twice the value of TML.
- $C_{TML} = 4$  signifies RDT duration equal to four times the value of TML.

Two key insights can be generated from the results reported in Table 2:

<sup>6</sup> The true value of  $\beta$  signifies the experimentally-derived  $\beta$  value, which is the slope of the Weibull probability plot.



- (a) For a given value of  $C_{TML}$ : the larger the value of  $\beta$ , the smaller would be the calculated value of  $N'$ .
- (b) For a given value of  $\beta$ : the longer the RDT duration (expressed in terms of  $C_{TML}$ ), the smaller would be the calculated value of  $N'$ . Here, the benefit of reducing *the value of  $N'$*  has to be weighed against potential costs associated with extending the test duration.

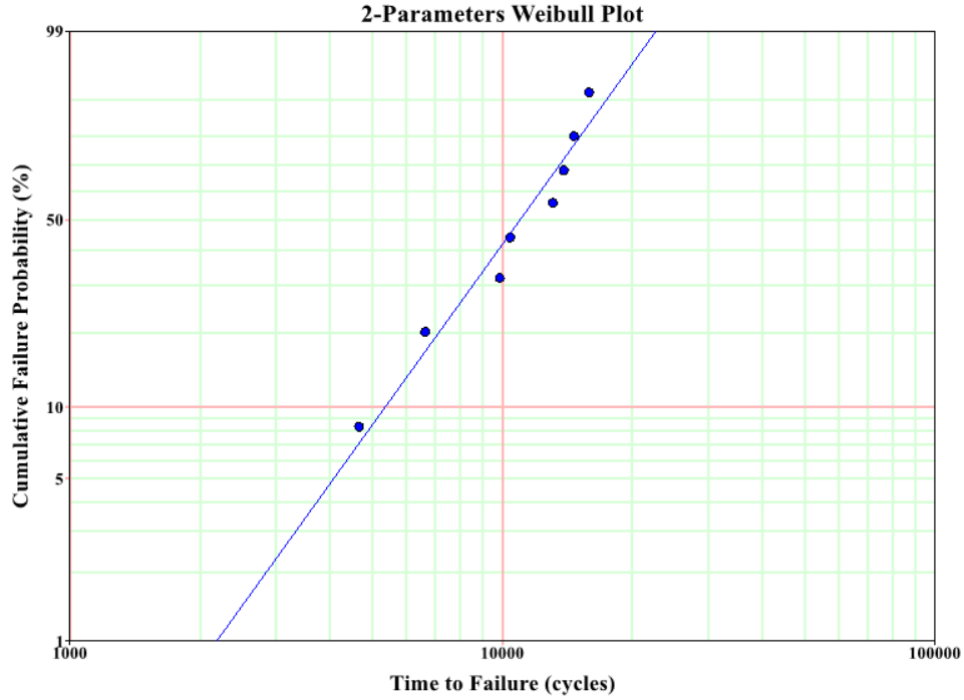
As discussed in subsection 2.5, the value of  $\beta$  could be assumed based on prior technical knowledge of proxy systems (*i.e.*, surrogates), existing field failure data, or using the physics-based reliability models. However, failure data from RDT can be also be used to generate a true value of  $\beta$ . It should not come as a surprise that the experimentally-derived  $\beta$  value may not be the same as the assumed  $\beta$  value. In such cases, the author of this work recommends repeating RDT at least three times to generate more sets of failure data points to obtain a range of experimentally-derived  $\beta$  values (which are the slopes of the corresponding Weibull probability plots). If the assumed  $\beta$  value is reasonably selected, it should lie within the experimentally-identified range. Alternatively, statistical tools could be used to perform uncertainty analysis to derive the lower and upper bounds of  $\beta$  at 90% or 95% *CL*. Example 1 is offered here to illustrate the aforementioned discussion.

**Example 1:** Assumed vs. true (*viz.*, experimentally-derived)  $\beta$  value

In this example and based on information provided in the case study (Subsection 3.1), the results of RDT is assumed to show that 8 out the 10 units on test failed before reaching the required 17,617 test cycles.<sup>7</sup> The two test units that did not fail (*i.e.*, right censored), have successfully completed the required 7,617 test cycles. The 8 units on test failed after the following number of cycles: 4,672; 6,645; 9,876; 10,443; 13,110; 13, 890; 14,655; 15,883 (refer to Table 7). These failure data are used to generate the Weibull probability plot as shown in Fig. 4. The 2-parameters Weibull distribution has been used to describe the statistical properties of the aforementioned failure data.

---

<sup>7</sup> The 17,617 test cycles are calculated using Eq. (10) for *LD* operational mode at 95% *CL*,  $\beta = 3.5$ ,  $N' = 10$ , and  $FPD_{avg} = 5E-3$ .



**Fig. 4.** Weibull probability plot of RDT results (refer to Example 1).

The y-axis in Fig. 4 represents the cumulative failure probability  $F(t)$  and can be described by Eq. (14) [28].

$$F(t) = 1 - \exp\left\{-\left(\frac{t}{\eta}\right)^\beta\right\} \quad (14)$$

Where  $\beta > 0$  and  $\eta > 0$

Based on Fig. 4, the calculated parameters of the Weibull model are:  $\beta = 2.6$  and  $\eta$  (*viz., the characteristics life, or scale parameter, at 63.2% cumulative failure probability*) = 12,646 cycles

Using Weibull++ from Reliasoft<sup>8</sup> (note that other statistical packages like Minitab<sup>9</sup> can also be used to provide this information), uncertainty bounds for  $\beta$  and  $\eta$  can be calculated as shown in Table 3.

<sup>8</sup> <https://www.reliasoft.com/Weibull/>

<sup>9</sup> <http://www.minitab.com/>

**Table 3**

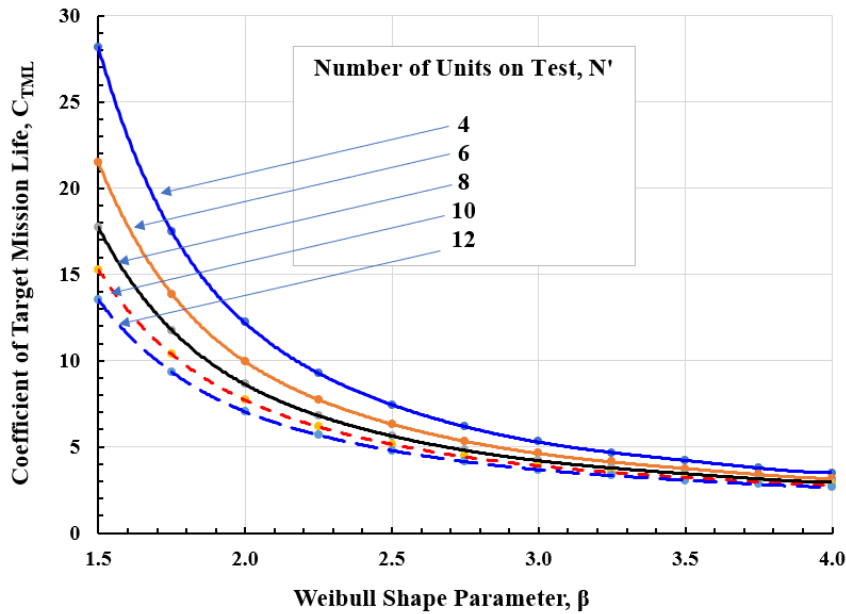
Statistics of Weibull parameters ( $\beta$ ,  $\eta$ ) with 95% confidence level (calculations are performed using ReliaSoft Weibull++ platform).

Weibull Parameters	Lower Bound (2.5%)	Mean	Upper Bound (97.5%)
$\beta$	1.4	2.6	4.8
$\eta$ (cycles)	9,469	12,646	16,889

Clearly the assumed  $\beta$  value of 3.5 is higher than the experimentally-derived mean  $\beta$  value of 2.6, however, it remains within the range of plausible values of  $\beta$  produced by RDT test data (Table 3). Also, the experimentally-derived mean value of  $\beta$ , statistically-derived lower and upper bounds, and the assumed value all are greater than 1.0 and, henceforth, the observed failures should pertain to the third region of the bath-tub curve (Fig. 2).

In the absence of experimental failure data, an assumed  $\beta$  value should suffice given that it is based on prior technical knowledge about the  $\beta$  values of surrogate systems, presence of historical field failure data, or predictions using physics-based reliability models.

Fig. 5 shows the impact on RDT duration (expressed in terms of the coefficient  $C_{TML}$ ) of the number of units in test,  $N'$ , and range of  $\beta$  values from 1.5 to 4.0. As can be seen, for a given value of  $N'$ , the test duration decreases as the value of  $\beta$  increases. For a given value of  $\beta$ , RDT duration decreases as the number of units on test,  $N'$ , increases.



**Fig. 5.** Dependence of RDT duration (expressed as multiples of TML,  $C_{TML}$ ) on  $\beta$  and  $N'$ .

### 3.3 Impact of $CL$ on RDT plan

Product reliability predictions with high  $CL$  reduce the risk ( $1 - CL$ ) of failing to achieve the stated or target reliability and, henceforth, could be desirable from both the producers and users' standpoints. However, higher  $CL$  come at a cost of increasing RDT duration (which could be expressed in number of testing hours or number of required test cycles). Table 4 shows how  $CL$  value impacts RDT duration (expressed in cycles). The results displayed in Table 4 are based on the following assumptions:

- Number of units of test,  $N' = 10$
- Weibull shape parameter,  $\beta = 3.5$
- TMR = 99.50%
- TML = 15 years or equivalently 5,475 cycles (based on 365 cycles/year).
- Zero-failures allowed RDT decision criterion.

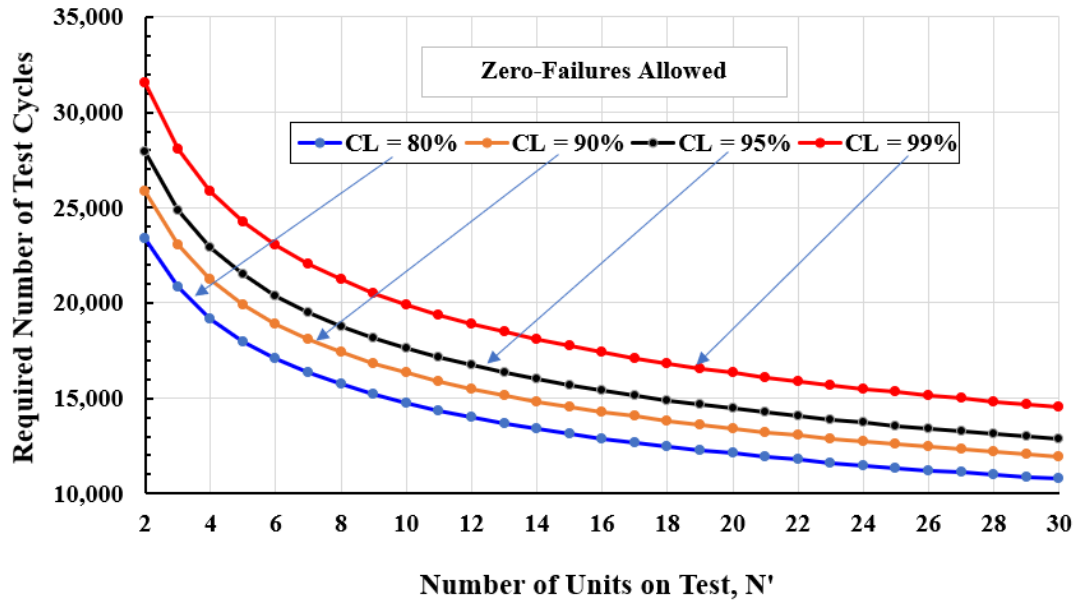
**Table 4**

Impact of increasing the confidence level on the required number of test cycles.

Confidence Level ( $CL$ )	Required Number of Test Cycles
70%	13,578
75%	14,136
80%	14,752
85%	15,462
90%	16,341
95%	17,617
99%	19,920

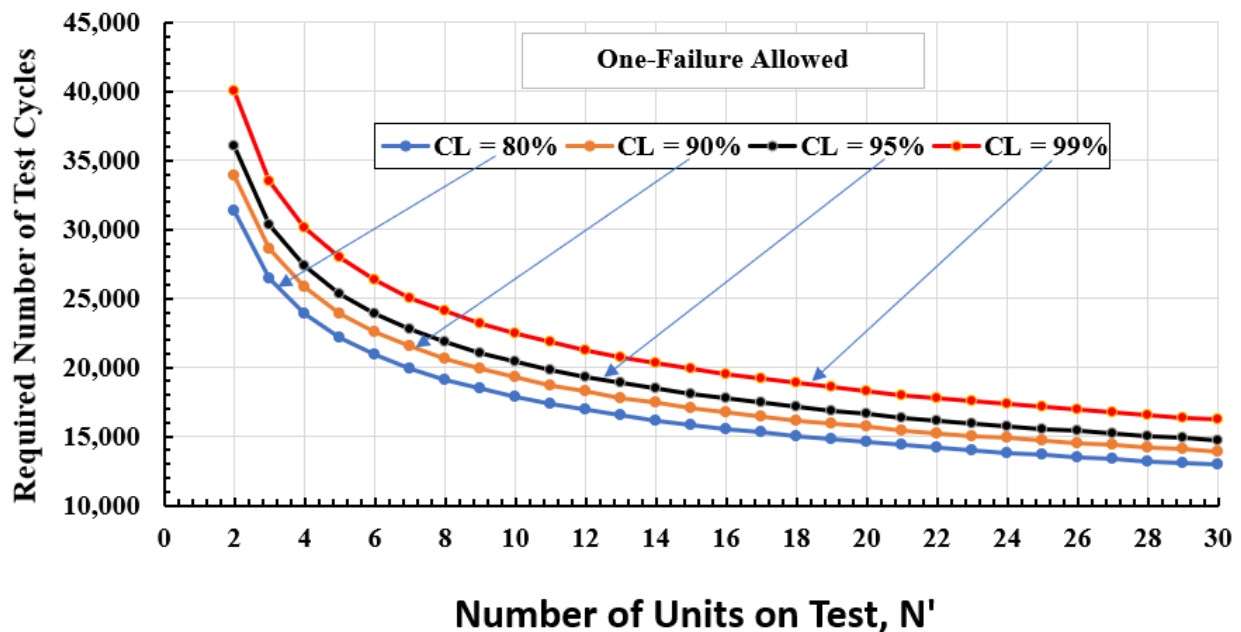
As can be seen in Table 4, increasing  $CL$  from 80% to 95% would result in 2,865 increase in required test cycles. The increase in number of required test cycles is associated with increase in testing duration, monitoring the units on test and, accordingly, the cost and schedule of releasing the new product design.

For the case of zero-failures allowed RDT plan, Fig. 6 shows the effect on required number of test cycles of a range of values of  $N'$  from 2 units up to 30 units with an increment of 2 units, given different values of  $CL$ .



**Fig. 6.** Effect of confidence level on relationship between number of units on test and calculated required number of test cycles (for zero-failures allowed, TMR = 99.50% and TML = 15 years or equivalently 5,475 cycles).

For the case of one-failure allowed RDT decision criterion, Fig. 7 shows the effect on required number of test cycles of a range of values of  $N'$  from 2 units up to 30 units with an increment of 2 units, given different values of the confidence level (CL).



**Fig. 7.** Effect of confidence level on relationship between number of units on test and calculated required number of test cycles (one-failure allowed, TMR = 99.50% and TML = 15 years or equivalently 5,475 cycles).

Both Figs. 6 and 7 show the same trend of variability of calculated number of test cycles with number of units on test, given different  $CL$  from 80% up to 99%. The following insights can be drawn from these two figures:

- For any given  $CL$ , the required number of test cycles can be reduced by increasing the number of cycles on test,  $N'$ . For example, Fig. 6 shows that for the zero-failure allowed RDT at 95%  $CL$ , the required number of test cycles can be reduced from 17,617 cycles at  $N' = 10$  units to 14,452 test cycles at  $N' = 20$  units. This reduction in test cycles represents ca. 18%.
- For a given number of units on test ( $N'$ ), reducing  $CL$  will result in reduction in the required test cycles. For example, Fig. 7 shows that for the one-failure allowed RDT decision criterion and  $N' = 10$  units, reducing  $CL$  from 95% to 80% will reduce the required number of test cycles from 20,406 to 17,889 test cycles (which is ca. 12% reduction in test cycles).

### ***3.4 Impact of LD vs. HD mode of operation on RDT duration***

Example 2 is designed to quantitatively demonstrate the impact of SIS operational mode (low- vs. high-demand) on the calculated RDT duration (expressed in multiples of TRL and test cycles).

#### **Example 2: Impact SIS operational mode (*LD* and *HD*) on RDT duration**

*Assumptions:*

- Number of units on test,  $N' = 10$  units
- $TML$  (viz., SIS design life) = 15 years = 5,475 cycles (based on 365 cycles/year)
- $R_{TML} = 99.50\%$ . That is to say, SIS average probability of failure on demand at TML is to be no more than 0.5%
- $CL$  used in reliability predictions = 95%
- Weibull shape parameter,  $\beta = 3.5$

Based on the abovementioned assumptions of Example 2, Table 5 summarizes the calculated values of  $C_{TML,LD}$  and required number of test cycles for the four SIL ratings described in IEC 61508-1 (refer to Table 1) and for *LD* mode of operation. Table 6 summarizes the calculated values of  $C_{TML,HD}$  and number of test cycles for the four SIL ratings described in IEC 61508-1 (refer to Table 1) and for *HD* mode of operation.

**Table 5**

Calculated values of  $C_{TML,LD}$  and required number of test cycles vs. SIL ratings for *LD* mode of operation.

SIL ratings per IEC 61508-1	<i>LD</i> Mode of Operation	
	$C_{TML,LD}$ Eq. (10)	Required number of test cycles
<b>SIL 4</b>		
Lower bound $FPD_{avg} = 10^{-5}$	19.01	104,084
Upper bound $FPD_{avg} = 10^{-4}$	9.85	53,909
<b>SIL 3</b>		
Lower bound $FPD_{avg} = 10^{-4}$	9.85	53,909
Upper bound $FPD_{avg} = 10^{-3}$	5.10	27,919
<b>SIL 2</b>		
Lower bound $FPD_{avg} = 10^{-3}$	5.10	27,919
Upper bound $FPD_{avg} = 10^{-2}$	2.64	14,442
<b>SIL 1</b>		
Lower bound $FPD_{avg} = 10^{-2}$	2.64	14,442
Upper bound $FPD_{avg} = 10^{-1}$	1.35	7,380

**Table 6**

Calculated values of  $C_{TML,HD}$  and required number of test cycles vs. SIL ratings for *HD* mode of operation.

SIL ratings per IEC 61508	<i>HD</i> Mode of Operation	
	$C_{TML,HD}$ Eq. (11)	Required number of test cycles
<b>SIL 4</b>		
Lower bound $FPH_{avg} = 10^{-9}$	19.74	108,097
Upper bound $FPH_{avg} = 10^{-8}$	10.23	55,988
<b>SIL 3</b>		
Lower bound $FPH_{avg} = 10^{-8}$	10.23	55,988
Upper bound $FPH_{avg} = 10^{-7}$	5.30	28,995
<b>SIL 2</b>		
Lower bound $FPH_{avg} = 10^{-7}$	5.30	28,995
Upper bound $FPH_{avg} = 10^{-6}$	2.74	15,001
<b>SIL 1</b>		
Lower bound $FPH_{avg} = 10^{-6}$	2.74	15,001
Upper bound $FPH_{avg} = 10^{-5}$	1.40	7,679

Two key insights to be gained from the results displayed in Tables 5 and 6 as follows:

- For any given SIL rating, number of units on test and  $CL$ , the required number of test cycles is higher for SIS functions with a  $HD$  mode of operation compared to SIS functions with a  $LD$  mode of operation. For example, for SIL 2 rating and  $HD$  mode of operation at lower bound  $FPH_{avg}$  of  $10^{-7}$ , the required number of test cycles is 28,995 (per Table 6). However, for SIL 2 rating and  $LD$  mode of operation at lower bound  $FPD_{avg}$  of  $10^{-3}$ , the required number of test cycles is 27,919 (per Table 5).
- For the zero-failures allowed RDT plans (which is primarily considered in this study), lack of clarity of the SIS function, *viz.*, being a  $LD$  vs.  $HD$  function would lead to either overestimating or underestimating the required number of test cycles. Note that overestimation of the required number of test cycles leads to a conservative but still valid zero-failures allowed RDT plan. To the contrary, underestimation of the required number of test cycles leads to an invalid zero-failures allowed RDT plan.

### 3.5 Impact of number of failures allowed in RDT plans on demonstrated reliability

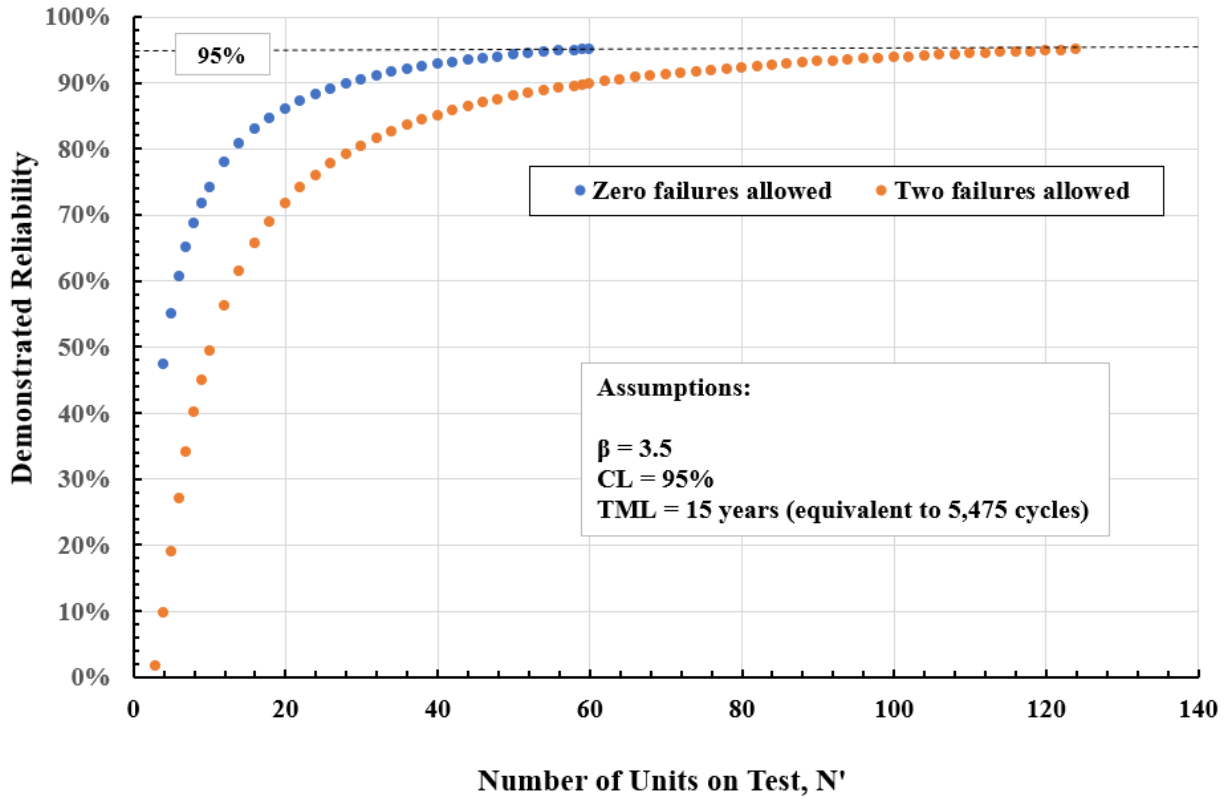
In this subsection, example 3 is intended to quantitatively demonstrate the impact of number of units on test,  $N'$ , on the demonstrated reliability for zero-failures allowed and two-failures allowed in RDT plans.

**Example 3: Impact of number of failures allowed in RDT plans on demonstrated reliability**  
Assumptions:

- TML = 15 years (or equivalently, 5,475 cycle)
- Weibull shape parameter ( $\beta$ ) = 3.5
- $CL$  = 95%

Based on stated assumptions, Fig. 8 shows the demonstrated reliability as a function of the number of units on test,  $N'$ , for zero-failure allowed and two-failures allowed RDT plans. One key statistical insight to be drawn from example 3 results (as displayed in Fig. 8) is that for any given demonstrated reliability, more test units would be required if one or more failures are allowed in RDT plans compared to RDT plans with zero-failures allowed. As Fig. 8 shows, to achieve 95% reliability with zero allowed failures, the number of units on test would be 60 units. However, with two allowed failures the number of units on test would increase to 124 units.





**Fig. 8.** Demonstrated reliability as a function of the number of units on test,  $N'$ , for zero-failure allowed and two-failures allowed RDT plans.

### 3.6 Formulation of SIS mission reliability statement

Example 4 demonstrates how the SIS mission reliability statement (MRS) can be articulated in a succinct and informative fashion.

#### Example 4: Formulation of SIS mission reliability statement

In this example, RDT has been performed for a new SIS design in order to validate whether the target reliability requirements can be achieved at the end of design life.

Data provided in this example - The RDT plan employed 10 units on test that were subjected to accelerated on/off power cycling as the imposed stressor. The required TMR is 99.5% which corresponds to  $FPD_{avg}$  of  $5 \times 10^{-3}$ . TML was assumed to be 5,475 cycles (viz., 15 year at 365 cycles per year). Per Table 1, this average failure probability corresponds to SIL-2 rating of SIS with a LD mode of operation. Reliability predictions should be made with 95% CL.

Under the stated conditions and assuming a *zero-failures* allowed RDT decision criterion and  $\beta$  of 3.5, each of the tested 10 units has successfully passed the required 17,617 cycles without failure.<sup>10</sup>

<sup>10</sup> The 17,617 test cycles are calculated using Eq. (10) for low-demand operational mode at 95% CL,  $\beta = 3.5$ ,  $N' = 10$ , and  $FPD_{avg} = 5E-3$ .

According to the stated RDT results, the SIS mission reliability statement can be formulated as follows:

*If 10 test units are cycled for 17,617 cycles and none of these units on test failed before meeting the stated number of test cycles, then the target mission reliability of 99.50% at 5,475 cycles target deign life can be achieved with 95% confidence level.*

### 3.7 Target mission life vs. demonstrated mission life

Herein, example 5 is intended to illustrate the difference between TML and DML.

#### Example 5: Target mission life (TML) vs. demonstrated mission life (DML)

Assumptions: same as in example 4 in subsection 3.6.

RDT test data: Unlike example 4 where it is assumed that all test units passed the zero-failures allowed RDT, example 5 involves failure of 8 out of the 10 tested units. The RDT results are summarized in Table 7.

**Table 7**

Example 5 RDT results.

Test Unit #	Passed / Failed	Measured Number of Test Cycles
1	Passed	Completed 17,617 tests cycles without failure
2	Failed	6,645
3	Failed	13,110
4	Passed	Completed 17,617 tests cycles without failure
5	Failed	15,883
6	Failed	13,890
7	Failed	4,672
8	Failed	10,443
9	Failed	14,655
10	Failed	9,876

Inspection of the results in Table 7 shows that the limiting number of test cycles to failure is 4,672 cycles and corresponds to test unit #7.

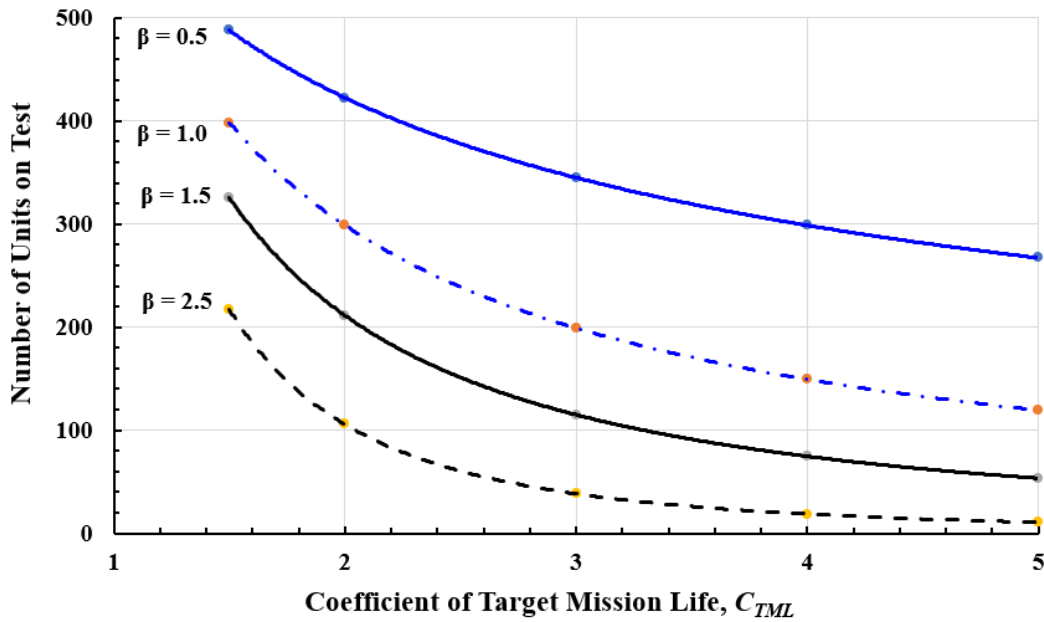
Using the assumed  $\beta$  value of 3.5, in order to meet TMR of 99.50%, the demonstrated mission life at 95%  $CL$  would be 1,452 cycles,<sup>11</sup> or ca. 4 years (which is ca. 25% of TML).

<sup>11</sup> This value has been calculated using Eq. (8) where  $\beta = 3.5$ ,  $N' = 10$ ,  $R = 99.5\%$ ,  $CL = 95\%$ . The calculated  $C_{TML}$  = 3.218 and, hence, the demonstrated mission life (DML) = 4,672 cycles to failure / 3.218 = 1,452 cycles = 1,452 cycles / 365 cycles per year  $\approx$  4 years.

### 3.8 Impact of RDT duration on calculated number of units on test, $N'$

RDT duration can be expressed as multiples of TML, *viz.*, the coefficient  $C_{TML}$ . As stated in the description of the case study (Subsection 3.1), SIS is assumed to experience 365 cycles/year and for TML of 15 years, the equivalent TML in cycles would be 5,475 cycles. Accordingly, for  $C_{TML} = 2$ , RDT duration would be 10,950 cycles and for  $C_{TML} = 4$ , RDT duration would be 21,900 cycles and so on.

The results displayed in Fig. 9 are generated using Eq. (5) to calculate  $N'$  values (y-axis) for different values of  $\beta$ , given a range of values for  $C_{TML}$  (X-axis) from 1.0 to 5.0 at  $CL = 95\%$  and TMR of 99.5%.



**Fig. 9.** Impact of zero-failures test duration on the calculated number of units on test,  $N'$ .

As Fig. 9 shows for any given value of  $\beta$ , the calculated number of units on test  $N'$  decreases as the test duration increases (expressed in multiples of TML, *viz.*,  $C_{TML}$ ). For example, for  $\beta = 2.5$  the number of test units decreases from 217 units at  $C_{TML}$  of 1.5 to 38 units at  $C_{TML}$  of 3, *viz.*, ca. 82% reduction on the number of test units. Moreover, for any give value of  $C_{TML}$ , the number of required test units decreases as the  $\beta$  value increases. For example, at  $C_{TML}$  of 2 using a  $\beta$  value of 2.5 in lieu of 1.5 would decrease the number of units on test from 211 units to 106 units, *viz.*, ca. 50% reduction in the number of required test units.

## 4. Conclusions

Reliability demonstration tests (RDT) are used in many industrial applications including printed circuit boards (PCB) and safety-related systems to guide decisions on qualifying and

certifying new product designs. Herein, new statistical formulations have been developed to assist reliability practitioners in designing efficient RDT plans for new designs of safety instrumented systems (SIS) subject to IEC 61508-1 (2010) requirements at low- and high-demand operational modes. An at-a-glance framework of the proposed statistical approach is provided to describe the logical steps to be followed to design an RDT plan and formulate the SIS mission reliability statement (MRS).

For given values of Weibull shape parameter ( $\beta$ ), confidence level ( $CL$ ), and target mission reliability (TMR) at the end of SIS design life, the following principal insights are identified:

- If all units on test ( $N'$ ) passed the zero-failures allowed RDT decision criterion, then the demonstrated mission life (DML) becomes equal to the target mission life (TML). (*See Example 4 for quantitative demonstration of this insight*).
- If one or more of  $N'$  did not pass the zero-failures allowed RDT decision criterion, then the DML is calculated using the limiting (*viz.*, smallest) number of test cycles to failure. In such case, DML should be less than TML. (*See Example 5 for quantitative demonstration of this insight*).
- It is possible to reduce  $N'$  by increasing the duration of the zero-failures allowed RDT. (*See Fig. 9 in subsection 3.8 for quantitative demonstration of this insight*).

In addition to the aforementioned insights, reliability practitioners need to carefully select a proper  $CL$  when designing RDT plans and conducting associated statistical calculations. Use of an overly conservative  $CL$  (*e.g.*, 99% instead of 90%) will unduly increase  $N'$  for a given RDT duration and vice versa (*viz.*, will increase RDT duration for a given value of  $N'$ ). Also, a lack of clarity regarding whether the SIS function should be considered a low-demand vs. high-demand safety function will lead to either underestimations or overestimations of the required  $N'$  or RDT duration. Finally, assuming a lower  $\beta$  value than its true value (*e.g.*, a  $\beta$  value of 2 instead of 3) will result in unnecessarily overestimation the required  $N'$  or RDT duration.

## Acknowledgements

The author of this work would like to thank the Fellow Librarians of the Bodleian Library at the University of Oxford in Great Britain for providing several of the literature material being reviewed during preparation of this manuscript. This author is also grateful to thorough reviews and constructive comments provided by his colleagues at Yale University in the U.S.

## References

- [1] Yang, G. (2009). Reliability demonstration through degradation bogey testing. *IEEE Transactions on Reliability*, 58 (4), 604-610.

- [2] Lipson, C., Sheth, N. (1973). Statistical Design and Analysis of Engineering Experiments. McGraw-Hill Book Company, New York.
- [3] Meeker W.Q. and Escobar, L.A. *Statistical Methods for Reliability Data*. New York: Wiley, 1998.
- [4] Leemis, L.M. (2006). Lower system reliability bounds from binary failure data using bootstrapping,” *J. Quality Technol.*, 38, 2–13.
- [5] Guo, H., Honecker, S., Mettas, A., and Ogden, D. (2010). Reliability estimation for one-shot systems with zero component test failures. *Proceedings Annual Reliability and Maintainability Symposium*, 2010.
- [6] Lawless, J.F. *Statistical Models and Methods for Life Time Data*, 2<sup>nd</sup> ed. New York: Wiley, 2003.
- [7] Hahn, G.J. and W. Q. Meeker, W.Q. *Statistical Intervals: A Guide for Practitioners*. New York: Wiley, 1991.
- [8] McKane, S.W., Escobar, L.A., and Meeker, W.Q. (2005). Sample size and number of failure requirements for demonstration tests with log-location-scale distributions and failure censoring. *Technometrics*, 47 (2), 82-190.
- [9] Feyzioglua, O., Altinel, I.K., and Özekici, S. (2006). The design of optimum component test plans for system reliability. *Computational Statistics & Data Analysis*, 50, 3099–3112.
- [10] Idris, M.R. and Aladin, A. (2013). Design an effective reliability demonstration test plan using six sigma approach. *Proceedings of the 2013 IEEE IEEM*, 1484-1488.
- [11] Luo, W. et al. (2015). Accelerated reliability demonstration under competing failure modes. *Reliability Engineering and System Safety*, 136, 75–84.
- [12] Lu, L. et al. (2016). Multiple objective optimization in reliability demonstration tests. *Journal of Quality Technology*, 48 (4), 326-342.
- [13] Li, P., Li, C. and Dang, W. (2017). Accelerated reliability demonstration testing design based on reliability allocation of environmental stresses. *Qual. Reliab. Engng. Int.*, 33, 1425–1435.
- [14] Kumar, M. and Bajeel, P.N. (2018). Design of component reliability test plan for a series system having time dependent testing cost with the presence of covariates. *Computational Statistics*, 33 (3), 1267–1292.
- [15] Altinel, I.K. (1994). The design of optimum component test plans in the demonstration of system reliability. *European Journal of Operational Research*, 78, 318-333.

- [16] Stone, G.C. and Van Heeswijk, G. (1977). Parameter estimation for the Weibull distribution, *IEEE Trans. On Elect Insul.* Vol EI-12, No-4, August, 1977.
- [17] Lu, M.W. and R. J. Ruddy, R. J. (2001). Laboratory reliability demonstration test considerations. *IEEE Trans. Reliability*, 50 (1), 12–16.
- [18] Hahn, G.J., Meeker, W.A. and Doganaksoy, N., (2003). Speedier reliability analysis. *Quality Progress*, 36 (6), 58-64.
- [19] Meeker, W.Q., Hahn, G.J., and Doganaksoy, N. (2004). Planning life tests for reliability demonstration. *Quality Progress*, 80–82.
- [20] Xingqiong, Y. and Lin, W. (2009). Reliability Demonstration Testing Procedure for Weibull Distribution about Zero Failure-data. *First International Workshop on Database Technology and Applications*, IEEE Computer Society, 68-71. DOI 10.1109/DBTA.2009.124.
- [21] Bhattacharya, P. and Mukhopadhyay, S. (2011). Weibull distribution for estimating the parameters and application of Hilbert Transform in case of a low wind speed at Kolaghat. *Int. J. of Multiphysics*, 5 (3), 203-214.
- [22] Guo, H. and Liao, H. (2012). Methods of reliability demonstration testing and their relationships. *IEEE Transactions on Reliability*, 61 (1), 231-237. DOI: 10.1109/TR.2011.2167782.
- [23] Rogers, S. and Kellner, D. (2015). Reliability Demonstration Testing: Can We Afford 80% Confidence? *2015 Annual Reliability and Maintainability Symposium*, 1-4.
- [24] Lee, Y-Li, et al. (2015). Durability reliability demonstration test methods. *Procedia Engineering*, 133, 31-59.
- [25] Klyener, A. and Sandborn, O. (2008). Minimizing life cycle cost by managing product reliability via validation plan and warranty return cost. *Int. J. Production Economics*, 112, 796-807.
- [26] IEC 61508-1:2010 (Edition 2.0). Functional safety of electrical/electronic/programmable electronic (E/E/ES) safety-related systems - Part 1: General requirements. Source: <http://www.iec.ch/functionalsafety/standards/>
- [27] IEC 61511-1: 2016(Edition 2.0). Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software application programming requirements.
- [28] Weibull++ (2014). User's guide (version 9). ReliaSoft Publishing. Source: [http://www.synthesisplatform.net/WeibullALTA/en/UG\\_WeibullALTA9.pdf](http://www.synthesisplatform.net/WeibullALTA/en/UG_WeibullALTA9.pdf)
- [29] Modarres, M., Kaminskiy, M.P., and Krivtsov, V. (2016). Reliability engineering and risk analysis: A practical guide. Third edition, ISBN 9781498745871, CRC Press.

- [30] Elsayed, E.A., (2012). Reliability Engineering. Second edition. ISBN 978-1-118-13719-2, John Wiley & Sons, Inc.
- [31] Barlow, R.E. and Proschan, F. (1975). Statistical theory of reliability and life testing: Probability models. ISBN 0-03-085853-4, Holt, Rinehart and Winston, Inc.
- [32] Yang, G. (2007). Life cycle reliability engineering. Hoboken, NJ, Wiley2007.
- [33] Elsayed, E.A. (2012). Overview of reliability testing. *IEEE Trans Reliability*, 61(2), 282–91.
- [34] Escobar, L.A. and Meeker, W.Q. (2006). A review of accelerated test models. *Stat Sci*, 21(4), 552–77.
- [35] Luo, W. et al. (2013). Reliability demonstration based on accelerated degradation testing for unknown model parameters. *Proc Inst Mech Eng., Part O.*, 227, 162–72.