Probability & Verification: Concepts & Principles

Objective

This write up defines the concepts (i.e., vocabulary and bolded words) and provides the principles (i.e., the relationship of one concept to another concept) that are the underpinnings to probabilistic thinking and system verification.

System Characteristics

A **system** is a set of interrelated components working together toward some common objective or purpose. **System characteristics** can be grouped into two categories: technical characteristics that address the system's functional capability and operating characteristics that address the system's operating outcomes. A system can serve its intended purpose most effectively when both its technical and operating characteristics are engineered into the design. For complex systems, both sets of system characteristics come from a variety of disciplines and are orchestrated by the systems-engineering process.

System functional capability is defined as the technical and physical characteristics (e.g., size, weight, volume, shape, accuracy, capacity, flow rate, throughput, units per time period, power output) the system (when operating) must exhibit to accomplish its intended function. **System operating outcomes** are defined as the non-technical and non-physical characteristics the system (when operating) must exhibit to accomplish its intended function. These operational behaviors though abstract are still "design for" parameters with the major parameters being: Safety (freedom from accident and loss), Reliability (time to failure), Maintainability (time to repair or maintain), Availability (mission readiness), Usability (interfaces between human and hardware and human and software), Supportability and Serviceability (support and service through out the planned life cycle), Producibility (ease and economy of producing), Disposability (disassembly and disposal) and Affordability (life-cycle cost or total cost of ownership and not just system acquisition cost).

Validation And Verification

Verification is one aspect of testing a system's fitness for purpose. Validation is the complementary aspect. In particular,

- **Validation** addresses, "Are we building the right system?" That is, does the system do what the customer really requires?
- **Verification** addresses, "Are we building the system right?" That is, does the system conform to the specifications?

The overall checking process for validation and verification is often referred to as "**V & V**." The **verification process** consists primarily of three methods, namely, analysis, test, and inspection. The first two are most applicable to reliability. Ideally, all reliability requirements should be verified by test. However, when it is not practical to test full-up systems, testing should be conducted at the sub-system level and use analysis to determine if the full-up system meets its requirement.

Philosophically, **verification theory** (The Principle of Verification), proposed by the logical positivists of the Vienna Circle, states that "statements and judgments can be accepted as meaningful and valid only to the extent that they are verifiable by means of sense experience" [1] (i.e., empirical; dependent on evidence that is observable by the senses). Thus, if something cannot be empirically verified, it is meaningless. Example: The statement "It is raining" is meaningless unless there is a way whereby one could, in principle, verify whether or not it is in fact raining. This theory has radical consequences for traditional philosophy as it, if correct, would render much other philosophical work and foundations for decision making meaningless (e.g., metaphysics and ethics).

Probability & Verification: Concepts & Principles

Determinism Versus Probabilism

Managers' ability to make good decisions (e.g., pertaining to verification of requirements) can be enhanced when they are aware of their thinking style and the tool sets used to make decisions (i.e., think about your thinking). In a broad sense, the decision maker pulls from two schools of thought, namely, determinism and probabilism.

Determinism is the belief that every event, act, and decision is the inevitable consequence of antecedents (past events) that are independent of the human will. In other words, determinism is the philosophical proposition that every event, including human cognition and action, is causally determined by an unbroken chain of prior occurrences. No wholly random, spontaneous, mysterious, or miraculous events occur. **Probabilism** is the belief that probability (likelihood) is the adequate basis for belief and action, since certainty in knowledge cannot be attained. In theology and philosophy, probabilism holds that in the absence of certainty, probability is the best criterion.

Uncertainty

Uncertainty does not imply no knowledge, but it does imply the exact outcome is not completely predictable. Most observable phenomena contain a certain amount of uncertainty. For example, repeated measurements of physical items generate multiple outcomes with some outcomes more frequent than others. The occurrence of multiple outcomes without any pattern is described by terms as being uncertain, random, and stochastic. **Stochastic** comes from Greek meaning "to guess at, aim at a mark, or pertaining to conjecture." For example, if several "identical" specimens of a steel bar in a laboratory were loaded for a pull test until failure, each specimen would fail at different load values. The load capacity of the bar is therefore a random quantity and is formally called in mathematics a **random variable**. Formally, a random variable assigns a single numerical value to each outcome of an experiment. From a point of view of discrete events, a **stochastic point process** is isolated events occurring at instants distributed randomly over a time continuum.

Engineers have always recognized the presence of uncertainty in their designs. Traditionally, uncertain design parameters were approached by using deterministic methods such as safety factors and safety margins. A **safety factor** is the ratio (division) of the capacity of the system to the load placed on the system. Where as, a **safety margin** is the difference (subtraction) between the system capacity and the system load. Typically, safety factors and safety margins are derived from past experience, ignore the variability present in both the loads placed on a system and the system's ability to react to the load, and do not absolutely guarantee safety or satisfactory performance.

In general, since all parameters in engineering analysis and design have some degree of uncertainty, all may be considered to be random variables. These uncertainties in the system come from two sources, namely, qualitative (cognitive) and quantitative (non-cognitive). Cognitive or qualitative sources of uncertainty pertain to the vagueness of the problem arising from intellectual abstractions (e.g., definition of structural performance and human factors) and can be dealt with for example using fuzzy set theory. Non-cognitive or quantitative sources of uncertainty involve probabilistic methods. Sections that follow address these further.

Probability And Statistics

Probability as a discipline makes a conclusion about data from a sample based on the analyst's knowledge of the population. A **population** is the complete and entire collection of data on the system under study, and a **sample** is a subset of the population. **Statistics** as a discipline makes a conclusion about the population based on the analyst's knowledge of the sample. As with verifying requirements, inferring certain facts about the population (flight hardware) from the results found in a sample (test hardware) drawn from that population uses a process called **statistical inference**.

A **statistic** is a numerical measurement that describes some characteristic of a sample. A **probability** as a measure is the likelihood that some given event will occur and is assigned a value between 0 and 1. In practice, this number has to be estimated. As a best guess, the probability is stated as a number and is technically called a **point estimate** [e.g., Pr (ISS gyros in a minimum configuration working in flight with heaters not available for 7 thermal cycles) = 0.962 or 96.2%]. The uncertainty encountered due to the math model's parameter(s) is described by an interval and is technically referred to as an **interval estimate** or as a **confidence interval** (e.g., the probability is between 0.899 and 0.983 with 95% confidence).

Probability & Verification: Concepts & Principles

Risk And Uncertainty In Decision Making

The manner in which a system's requirement or specification is verified is similar to the types of decisions managers make—it depends on how much knowledge or information they have about the system. The quantity and quality of information available and understood by the decision maker generates three categories or environments for decision making[2], namely,

- **Decision Making Under Certainty** where the decision maker knows with certainty the consequence of every alternative or decision choice. Naturally, the decision maker will choose the alternative that will result in the best outcome. However, few managers are fortunate enough to have complete information or knowledge about the states of nature under consideration.
- **Decision Making Under Risk** where the decision maker knows the probability (likelihood) of occurrence of each outcome. Qualitatively, **risk** can be defined in three dimensions, namely, X is "what can go wrong," Y is "how likely is this to happen," and Z is "if it does happen, what are the consequences?" Quantitatively, risk = (hazard likelihood) x (hazard consequence). The Safety and Risk disciplines are the major contributors to identifying and describing the X and Z dimensions of risk. Where as, many of the quantitative techniques in the Reliability discipline determine the likelihood portion of risk since Y = 1 – reliability measure.
- **Decision Making Under Uncertainty** where the decision maker does not know the probabilities of the various outcomes. Genuine uncertainty, on the other hand, cannot be assigned such a (well grounded) probability. Furthermore, genuine uncertainty can often not be reduced significantly by attempting to gain more information about the phenomena in question and their causes.[3]

Uncertainty In Modeling

The knowledge state engineers and analysts have, both qualitatively and quantitatively, about a system will determine the degree of uncertainty. In any event, when models are used, the technical and management teams will experience uncertainty and will have to address it accordingly. Commonly in the Reliability Engineering discipline, there are three classes of uncertainty *, namely:

- **Intrinsic Uncertainty** – The variability obtained from measurement and from the nature of the test.
- **Model Uncertainty** – The lack of complete knowledge in being able to understand and or describe a system's response and its relationship to events and other systems, and the lack of accuracy (goodness of fit) in the selected (postulated) math model in being to properly describe the data.
- **Parameter Uncertainty** – The error possibly generated by using only sample data instead of population data to determine the value of the math model's parameter(s). A **parameter** is a numerical measurement that describes some characteristic (e.g., mean) of the population. Thus, when only sample data is used, the parameter is most likely not the true value for the parameter and is only an estimate. The more data that is available, the closer the parameter estimate as a point value (point estimate) is likely to be to the true value. The interval estimate (confidence interval) addresses only uncertainty in the parameter.

A math model will describe a specific system when the parameter(s) in the system's math model are loaded with specific numerical value(s). That is, a math model could, for example, have two parameters, namely, the average or mean-time-between-failure, **MTBF**, (e.g., $\theta = 10{,}000$ hours) and standard deviation (e.g., $\sigma = 100$ hours). In general, the larger the **sample size**, the more likely the parameter's point estimate will be closer to the true value and the length of the parameter's interval estimate will be smaller.

Example: For the mean-time-between-failure (θ) parameter with some assumed and specified math model, "Based on the sample data collected, there is a 0.95 probability, commonly stated as 95% confidence, that the interval estimate contains the true value for the parameter θ." This can be denoted as $\Pr(\theta_L \leq \theta \leq \theta_U) = 0.95 = 1 - \alpha$ where $\alpha = 0.05$ and α (alpha) is producer's risk, one of the two types of decision risks. For more on α and producer's risk, see the section entitled Tests of Statistical Hypotheses.

* Note: Typically, the Safety Engineering and probabilistic risk assessment (PRA) communities describe uncertainty as being either aleatory or epistemic.[4]

Probability & Verification: Concepts & Principles

- **Aleatory uncertainty** is physical variability. Aleatory uncertainty is the uncertainty and lack of confidence that originates from the physical variability in material properties or in the system. Aleatory uncertainty is *not* reduced by collecting more data and developing better analytical relationships. It is inherent to the material or system. Collecting more data will only allow the variability to be more precisely predicted. To reduce the aleatory uncertainty, the material has to be modified or the system changed. An **aleatory model** describes the randomness (variability) in the physical processes modeled. This uncertainty described by the model of the world is sometimes referred to as "randomness" or "stochastic uncertainty."
- **Epistemic uncertainty** is knowledge uncertainty. For example in Reliability estimation, epistemic uncertainty is the uncertainty and lack of confidence that originates from having a lack of data to estimate the reliability. Epistemic uncertainty is reduced by collecting more data and by developing better analytical relationships. An **epistemic model** represents the state of knowledge regarding the validity of the model assumptions and numerical values of the parameters. Epistemic models deal with non-observable quantities (e.g., failure rates and model assumptions).
- Example: Assume a graph has the y axis as the probability of success (i.e., reliability) and the x axis as time. The plotted curve is aleatory (since it deals with the observable quantity time) and the probability shown on the curve is epistemic.

Modeling System Operating Outcomes

When the verification process uses the analysis method, models are used in place of the actual physical test. Models can be of two types, namely, system models and mathematical (math) models.

- The **system model** describes the configuration and response of the system's hardware, software, orgware (human element). In failure space and in a "top-down" manner, these system elements and their relationships are commonly described by a master logic diagram, event trees, event sequence diagrams, and fault trees.
- The **math model** is the mathematical formula that describes or "models" the data pertaining to the phenomenon of interest (e.g., failures over time). For example, the Safety, Reliability, and Risk disciplines quantitatively describe a system's **operating times** (time intervals with no failure occurring) and **times to failure** (time intervals ending with a failure occurring) by math models called **lifetime distributions**, namely:
  - **Probability Density Function** (pdf), denoted **f(t)**, is the formula that describes (based on expert opinion or postulated from the failure data's histogram) the frequency or distribution of failures for a system (or system element) over the entire range of time. The larger the value of f(t), the more failures that occur in a small interval of time around t. The pdf is the basic model used for deriving other metrics and conducting in-depth analytical studies.
  - **Cumulative Distribution Function** (cdf), denoted **F(t)**, is the probability a system (or system element) will fail by a specified time t. It is the probability of failure, often interpreted as the population fraction *failing* by time t. Mathematically, $F(t) = \int f(t)dt$ with the limits on the integral ranging from $-\infty$ to t. However, when the pdf is the Exponential distribution or the Weibull distribution (as opposed to the Normal distribution), the lower time limit for the cdf starts at zero instead of negative infinity.
  - **Reliability (Survival) Function**, denoted **R(t)**, is often interpreted as the population fraction *surviving* time t. Mathematically, $R(t) = \int f(t)dt$ with the limits on the integral ranging from t to $+\infty$. Since R(t) is the probability of success (denoted $\mathbf{P_s}$) and F(t) is the probability of failure (denoted $\mathbf{P_f}$), then $R(t) + F(t) = 1$. In terms of the likelihood portion of the risk definition, $P_f = F(t) = 1 - R(t)$.
  - **Hazard Function**, denoted **h(t)**, is often called the hazard rate or failure rate. It measures the rate of change in the probability that a surviving system or system element will fail in the next small interval of time. It can be shown that $h(t) = f(t)/R(t)$.

Tests Of Statistical Hypotheses

A **hypothesis** is a statement (claim) that something is true (e.g., the system's performance is greater than the minimum specification of xxx). **Statistical hypotheses** (e.g., an assumption about the population being sampled) commonly found in verification, use confidence intervals or interval estimates to address uncertainty. However, confidence intervals address only one of the two types of errors that are possible in making incorrect decisions. That is, confidence intervals assist in preventing a type I error but not a type II error.

Probability & Verification: Concepts & Principles

- A **type I error** occurs when a "good" system fails the test. This type of error is referred to as **producer's risk** or **significance level of the test** and has a probability of occurrence denoted as **α** (alpha). Traditionally, α is set at a low level (e.g., 0.10, 0.05, 0.01, or 0.001).
- A **type II error** occurs when a "bad" system passes the test. This type of error is referred to as **consumer's risk** and has a probability of occurrence denoted as **β** (beta). There are no formal standards for statistical power; most researchers who assess the power of their tests use 0.80 as a standard for adequacy.
- The probability of not making a type I error is **$1 - \alpha$** and is referred to as the **confidence level of the test**.
- The probability of not making a type II error is **$1 - \beta$** and is referred to as the **power of the test**
- The α and β probabilities are often referred to as the risks of making incorrect decisions. One objective of hypothesis testing is to design a test such that the α and β risks are small.
- To decrease both α and β, the experiment (verification test) will need to increase the sample size. Traditionally, one step in hypothesis testing is the selection of α and not β. However, when α and β are both selected, the required sample size is then specified. And when only α is decreased, β is increased, and vice versa. In other words, not only does a decrease in α result in and increase in β, but the decrease in α increases the length of the confidence interval (called the **acceptance region** for hypothesis testing).

Hypothesis testing typically tests the negative version of the hypothesis. This negated hypothesis is called the **null hypothesis**, denoted **H_0**, and has a test result as either reject H_0 or fail to reject H_0. The hypothesis being the requirement to be verified is called the **research hypothesis** or **alternative hypothesis**, denoted either as **H_1** (or **H_a**), and is assumed to be true when the null hypothesis is false.

Since 100% of a population typically can not be tested, it can never be said for sure that a given hypothesis is true. Thus, a hypothesis can never be accepted, and the negative version of the hypothesis (H_0) is used to counter what is theorized. If a test indicates H_0 *can* be rejected with $1 - \alpha$ of statistical confidence, the tested theory (research hypothesis, H_1) is supported by default. If a test indicates H_0 *cannot* be rejected with $1 - \alpha$ of statistical confidence, the research hypothesis (H_1) is not supported by default.

Example: In the American justice system an accused is assumed to be not guilty (null) until he/she is proven to be not guilty beyond a reasonable doubt (some allowable risk level). If the accused is not proven guilt, he/she is not declared innocent since innocence has not been proven. The accused is declared to be "not guilty" since guilt has not successfully been proven.

The table below shows the relationship and the common and statistical terminology for all combinations of the possible realities of the hypothesis and the outcomes of the hypothesis test.

	The null hypothesis (H_0) is true. Thus, the research hypothesis (H_1) is <u>not</u> true.	The null hypothesis (H_0) is false. Thus, the research hypothesis (H_1) is true.
The decision maker rejects the null hypothesis (H_0). Thus, the research hypothesis (H_1) is assumed to be true.	Type I error = Producer's risk = **Wrong Decision**. $\Pr[\text{reject } H_0 \mid H_0 \text{ is true}]$ $= \Pr[\text{Type I error}] = \alpha$ = Significance level of the test.	**Correct Decision.** $\Pr[\text{reject } H_0 \mid H_0 \text{ is false}]$ $= 1 - \beta$ = Power of the test.
The decision maker accepts (technically, fails to reject) the null hypothesis (H_0). Thus, the research hypothesis (H_1) is assumed to be <u>not</u> true.	**Correct Decision.** $\Pr[\text{accept } H_0 \mid H_0 \text{ is true}] = 1 - \alpha$ = Confidence level of the test.	Type II error = Consumer's risk = **Wrong Decision**. $\Pr[\text{accept } H_0 \mid H_0 \text{ is false}]$ $= \Pr[\text{Type II error}] = \beta$.

<u>Note</u>: In sentence form, the cell in the upper-left-hand corner reads as follows: "A Type I error also known as producer's risk results in a wrong decision. The probability of rejecting the null hypothesis given that the null hypothesis is true is also known as the probability of a Type I error. Both mentioned probabilities are denoted by α, a Greek letter called alpha. Alpha is the risk level the decision maker selects in advance for this possible incorrect decision along with the sample size to be used in the test. This risk level is technically referred to by the Statistics community as the "significance level of the (hypothesis) test."

Verification Testing

The **verification and validation (V & V) phase** consists of two major steps: design verification and process validation. These two steps have the purpose to verify that the design achieves the requirements and specifications (e.g., reliability), to validate that the manufacturing and operations processes are capable, and to analyze and correct the failure modes and mechanisms of the system and system elements that failed during the verification and validation tests. The V & V phase begins after the design of the system has been successfully completed and a small number of prototypes are built for the design verification step. The **design verification** step primarily uses the analysis method, the testing method, or a combination. These two methods are commonly referred to as analytical verification and verification testing and will be described next.

Analytical verification, one of the two methods for design verification, is used when testing is not practical due to cost or time, when there is a need to validate an analytical model for use at a later time when testing is not possible or desired, and when there are adequate mathematical and system models that relate system performance (e.g., end of life) to stresses, design parameters, and manufacturing and operating variables. Analytical verification, called **virtual validation** in some industries, deploys a variety of techniques with some using extensive computer simulation and numerical calculation, namely, reliability-block-diagram analysis (RBDA), failure-modes-effects, and criticality analysis (FMECA), fault-tree analysis, worst-case analysis, sneak-circuit analysis, life-stress relationships (e.g., Arrhenius, Eyring, S-N curves), finite-element analysis, and probabilistic-risk assessment (PRA).

In some cases, formal mathematical (closed form) solutions are difficult or impossible to obtain. Under such conditions, it may be necessary to use a method known as **Monte Carlo simulation** or Monte Carlo analysis. The name itself has no significance except that it was used first by von Neumann during World War II as a code word for work related to the development of the atomic bomb. In brief, the Monte Carlo simulation method uses random numbers to solve certain stochastic or deterministic problems.

Verification testing, the other method used for design verification, demonstrates with minimum test time and sample size that the system satisfies the requirements and targeted specifications. Before testing begins for the design verification step, a **test plan** must be developed that specifies test conditions, sample sizes, acceptance criteria, and test operation procedures. At least for reliability purposes, both the design verification and process validation steps should use the same test stress types and levels. A large sample in design verification testing is often too costly; however, it should be large enough so that the evidence to confirm the design is statistically valid or at least balances the cost of testing with the risk of not testing. If a design fails during design verification testing, it must be revised—and the redesigned system must be subjected again to verification testing. This **test-analyze-and-fix (TAAF)** process being a very common practice (ref. reliability growth) can be a risk to both schedule and cost of the program—especially in a competitive environment. Therefore, it is vital to design-in reliability and to eliminate potential failure modes even before prototypes are built.

Before describing the different types of verification tests related to safety and mission assurance with an emphasis on reliability, it is important to mention that the V & V phase may not be the first time a system is tested. The system may have completed **accelerated life tests**, tests that subject test units to higher-than-nominal-use stress levels to shorten their times to failure. Accelerated life tests for example are used early in the design phase to assess and qualify materials and components and later in the design phase to perform robust design activities that choose the optimal settings for the design parameters. However, due to advancements in technology and manufacturing, it is not uncommon for accelerated life tests to yield no or few failures at low stress levels. In these situations it is difficult or impossible to analyze and assess system-element-life data and system interplays and make meaningful inferences about performance, safety, and mission assurance. However, it possible to infer reliability, for example, by analyzing degradation data. A **degradation test** directly relates reliability to physical characteristics and has several advantages over a life test, namely, it allows reliability to estimated even before a test unit fails (thus, shortens the test time) and often yields more accurate estimates especially when a test is highly **censored** (the test is terminated for some reason prior to allowing all units on test to fail).

The table below describes various tests for verifying **reliability**[a], the probability a system will perform its intended function without failure under specified conditions (environment) for a specified period of time (mission time).

Probability & Verification: Concepts & Principles

Reliability[a] Test	Sample Size & Test Time[b]	Comments (see table notes below)
Bogey (Requirement) Testing	Uses a predetermined sample size for a certain period of time. Requires a large sample size and/or extensive test length.	The required reliability is verified if no failures occur during the test. Easy to implement; does not require failure monitoring and performance measurement during testing. Protects only consumer's risk.
Sequential-Life Testing	Tests the samples one unit at a time until failure or until a pre-specified period of time has elapsed. Sample size is a random number but is smaller than the bogey test.	The accumulated test results are compared with the predetermined rules[c] to decide whether (1) Required reliability is achieved, (2) Required reliability is not achieved, or (3) The test is to be continued. Considers both consumer's risk and producer's risk.
Test-To-Failure Testing	Tests the samples until all fail—thus, testing often takes longer. Typically, requires fewer samples.	Provides accurate reliability predictions. Generates additional information since the test is usually conducted under accelerated conditions—thus, needs an appropriate acceleration relationship. For some system types, failure is defined in terms of a performance characteristic crossing a threshold.

Reliability Test Table Notes

a. It is **availability** and not reliability that addresses **downtime** (i.e., time for maintenance, repair, and replacement activities). Thus, prior to commissioning an analysis, it is helpful to communicate if the intent is limited to reliability or is it really availability. Availability is the probability that a system is operational, and availability is a function of both reliability and maintainability. As with reliability, availability can be either a demonstrated or predictive measure of performance. **Demonstrated availability** is simply (uptime)/(uptime + downtime). **Predictive availability** has three types, namely, at time t (**point availability**), over an interval from t_1 to t_2 (**interval availability**), or over the long run as $t \to \infty$ (**steady-state availability**). In addition, steady-state availability has three common forms (with each depending on the definitions of uptime and downtime), namely, inherent availability, achieved availability, and operational availability. **Inherent availability** is based solely on the failure (reliability) distribution and the downtime distribution (maintainability) and is an important system design parameter for trade studies.

b. Verifying high reliability at a high confidence level requires a large sample or a long test time. When neither is available, accelerated testing may be the best choice. However, care must be taken to ensure that elevated stress levels do not produce failure modes different from those intended in normal operation. Also, sample size can be reduced using the **Bayesian method** if there exists known prior information about the life parameter to be verified. Sometimes this prior information is available from accelerated tests conducted earlier in the design and development phases and/or from failure (problem reporting and corrective action) data of prior generation system elements.

c. For example, the test plan will specify the relationship between the true reliability (e.g., mean-time-between-failure, MTBF) of the system tested and the probability of acceptance by the plan. This relationship shown as a curve will plot consumer's risk (β) for various values of MTBF. This curve is used in sequential type verification tests and is called the **operating characteristic (OC) curve**.

■■■

Endnotes

1. Ideas of the Great Philosophers, William S. Sahakian and Mabel Lewis Sahakian, 1966, p. 156.
2. Quantitative Analysis for Management, 6th ed., Barry Render and Ralph M. Stair, 1997, p. 36.
3. "Modelling Society's Capacity to Manage Extraordinary Events," Anna-Lena Lövkvist-Andersen, Richard Olsson, Tom Ritchey, Maria Stenström, Paper presented at the SRA (Society for Risk Analysis) Conference in Paris November 15-17, 2004. http://www.swemorph.com/pdf/sra.pdf
4. Notes from Dr. William E. Vesely, NASA Headquarters, and from Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, version 1.1, NASA Office of Safety and Mission Assurance, 2002. http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf

References

Blanchard, Benjamin S. and Fabrycky, Wolter J., Systems Engineering and Analysis, 4th ed., Prentice Hall, 2005.

Ebeling, Charles E., Introduction to Reliability and Maintainability Engineering, Waveland Press, 2005.

Haldar, Achintya and Mahadevan, Sankaran, Probability, Reliability, and Statistical Methods in Engineering Design, John Wiley and Sons, 2000.

Hicks, Charles R., Fundamental Concepts in the Design of Experiments, 3rd ed., Saunders College, 1982.

Leemis, Lawrence M., Reliability Probabilistic Models and Statistical Methods, Prentice Hall, 1995.

Raheja, Dev and Allocco, Michael, Assurance Technologies Principles and Practices: A Product, Process, and System Safety Perspective, John Wiley and Sons, 2006.

Relex Software Corporation's Reliability Dictionary, http://www.relex.com/resources/reliabilitydictionary.asp

Triola, Mario F., Elementary Statistics, 4th ed., Benjamin/Cummins, 1989.

Yang, Guangbin, Life Cycle Reliability Engineering, John Wiley and Sons, 2007.

Probability & Verification: Concepts & Principles

Hardcopy Version: Index With Page Numbers (Locates only the definition and not all occurrences)

Probability & Verification: Concepts & Principles

Electronic Version: Index With Links (Locates only the definition; use “Edit” and “Find” to locate all occurrences)