What is Reliability?

- The Likelihood of Performance as Intended Over the Life Cycle (p_s) -

- The Likelihood of Potential Loss (1- p_s) -

Timothy C. Adams

NASA Kennedy Space Center

Engineering

Tim.Adams@NASA.gov

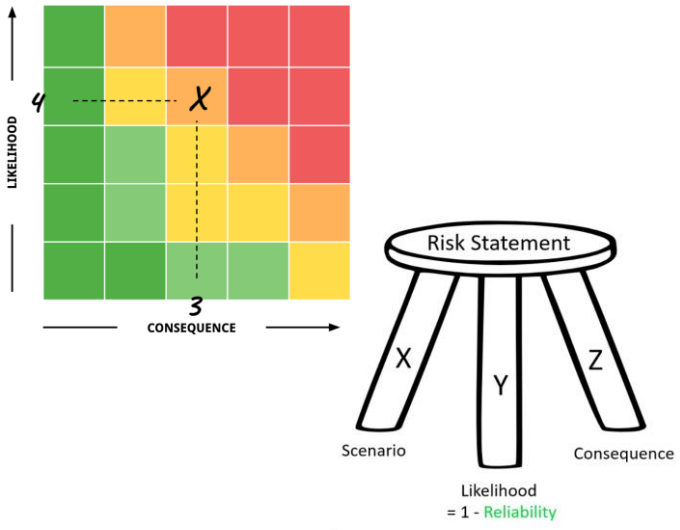
April 25, 2024

Table of Contents

Tim.Adams@NASA.gov

Prospectus

- Claim: We are not done with Reliability until we are done with Safety!
  - And if we continue to use a risk matrix, then we need to use it properly. Both axes (likelihood and consequence) of the risk matrix need adequate attention.
- Goal: Inform decision makers to embrace and use the Reliability discipline.
  - This is important for decisions under risk (and with uncertainty) since ...
  - **Actual Results = Planned Results +/- Risk**.
  - Risk is potential loss in failure space. "Potential" is the likelihood axis of the risk matrix.
  - The likelihood axis is the probability of failure (p_f) axis, and p_f = 1 - Reliability.
  - So, **what is reliability**?
- This presentation for Reliability provides:
  1. Fundamental concepts and relationships.
  2. Strategies to plan and make analytical products.
  3. Details on the required data.
  4. Resources to learn more and do more.
  5. Slides formatted for others to conduct training.
  6. Slides formatted as job aids for the practitioner.



Risk: Reliability Makes the Likelihood Component

Risk as a Concept

- Risk is:
  - Potential loss or potential gain.
  - The uncertain deviation (delta) in the execution of a management plan.
  - Resources:
    - ISO 31000, Risk Management
    - NPR 8000.4C, NASA Risk Management
- Risk when limited to potential loss (failure space) is:
  - A qualitative or quantitative estimate of the potential loss occurring due to natural or human activities.

Risk as an Operation

- Using both potential loss and gain:

  Actual results = Planned results +/- Risk

- **Risk statement** limited to potential loss:
  - **X**, Scenario: What can go wrong?
  - **Y**, Likelihood: What is the probability it will happen (p_f = 1 - **Reliability**)?
  - **Z**, Consequence: What is the impact if it did happen? For example, loss of ...
- **Risk measure** = **Y*Z** = (Likelihood)*(Consequence) being a:
  - Number (i.e., product) or
  - Graphic (i.e., point in a risk matrix).

Risk Likelihood (Y) = Probability of Failure (p_f) = Unreliability (U) = 1 - Probability of Success (p_s) = 1 - Reliability (**R**)

Risk Decisions (Handling, Responding): Accept (fight), Avoid (flight), Hold (freeze), Mitigate (change), and Transfer (share)

Engineering Assurance and the RMA Program

Safety: Freedom from accident and loss	**Usability**: Human factors (e.g., compatibility and interfaces)	**Supportability**: Service throughout the life cycle (e.g., support facilities and logistics)
Reliability: Likelihood of continuous uptime (no failures) for a stated mission and conditions	**Maintainability**: Likelihood that service returns failures to an uptime state by a certain time	**Availability**: Likelihood a repairable item will be in an uptime state; **A** = f (**R**, **M**)
Producibility: Ease and economy of producing or manufacturing	**Affordability**: Total cost of ownership and not only system acquisition cost	**Disposability**: Disassembly and disposal (environmental stewardship)

Engineering Assurance

- Identifies and addresses issues and hazards early (i.e., during design and not during operation).
- Is cross-functional; it works closely with other disciplines and functions (e.g., program management, chief engineers, design, and operations) over the life cycle.
- Is called **Specialty Engineering** by International Council on Systems Engineering (INCOSE).

The **Reliability-Maintainability-Availability Program** consists of integrated and sequenced tasks that are implemented throughout the item's life cycle. These tasks are customized to fit the needs of specific items. Resources:

- NASA-STD-8729.1, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems
- System Reliability Toolkit - V: New Approaches and Practical Applications, Quanterion, 2015
- Life Cycle Reliability Engineering, Yang, Wiley, 2007
- The Process of Reliability Engineering: Creating Reliability Plans That Add Value, Carlson & Schenkelberg, FMS Reliability, 2023

Definitions: R (↑) and its Counterparts M (↓) and A (↑ ↓)

Reliability (R)	Maintainability (M)	Availability (A)[2]
– The probability an item[1] will perform its intended function with no failure for a given time interval and under given conditions (e.g., environment and loads). – The probability an item will be in and remain in an uptime state.	– The probability a failed item[1] will be restored or repaired to a specified condition within a given time interval. – The probability a failed item (an item in a downtime state) will be returned to an uptime state within a given time interval.	– The probability a repairable item[1] will perform its intended function at a given point or interval of time when operated and maintained in a prescribed manner. – The probability a repairable item will be in an uptime state and will recover from downtime states. – A mathematical function of R and M, A = f (R, M).

[1] An **item** is hardware (Hw), software (Sw), orgware (Ow) or humans, interfaces, or combination.

[2] **System Availability** = $A_{Hardware} * A_{Software} * A_{Orgware} * A_{interfaces}$ where * denotes "and."

System Effectiveness is: (1) System Availability, (2) Dependability (i.e., operating condition, trustworthiness), and (3) Capability (i.e., meets mission demands).

Reliability Statements: Writing Quantitative Goals

- Tip: Use the **ABCD** mnemonic to write goals and requirements. Example:

Audience	The Federally mandated automobile catalytic converter …
Behavior	will perform its intended function with no failure …
Conditions	under specified driving situations with preventive maintenance for …
Degree	80,000 miles/8 years [*with 0.9999 probability and 95% confidence*].

- A **goal or requirement statement for reliability** (availability) contains:

  A = Item of Interest (i.e., hardware, software, orgware or humans, and/or interfaces) +

  B = Intended Function with no failure (with repair and service for availability) +

  C = Conditions (e.g., environment and loads) +

  D = Mission Duration + Probability of Success[1] + Statistical Confidence (Uncertainty).

[1] The "probability of success" portion of the goal statement for reliability (or availability) is commonly called reliability (or availability). However, this “short cut” is overly simplified and omits details to statistically make a claim or to verify.

Setting the Goal: How Many 9s Are Required?

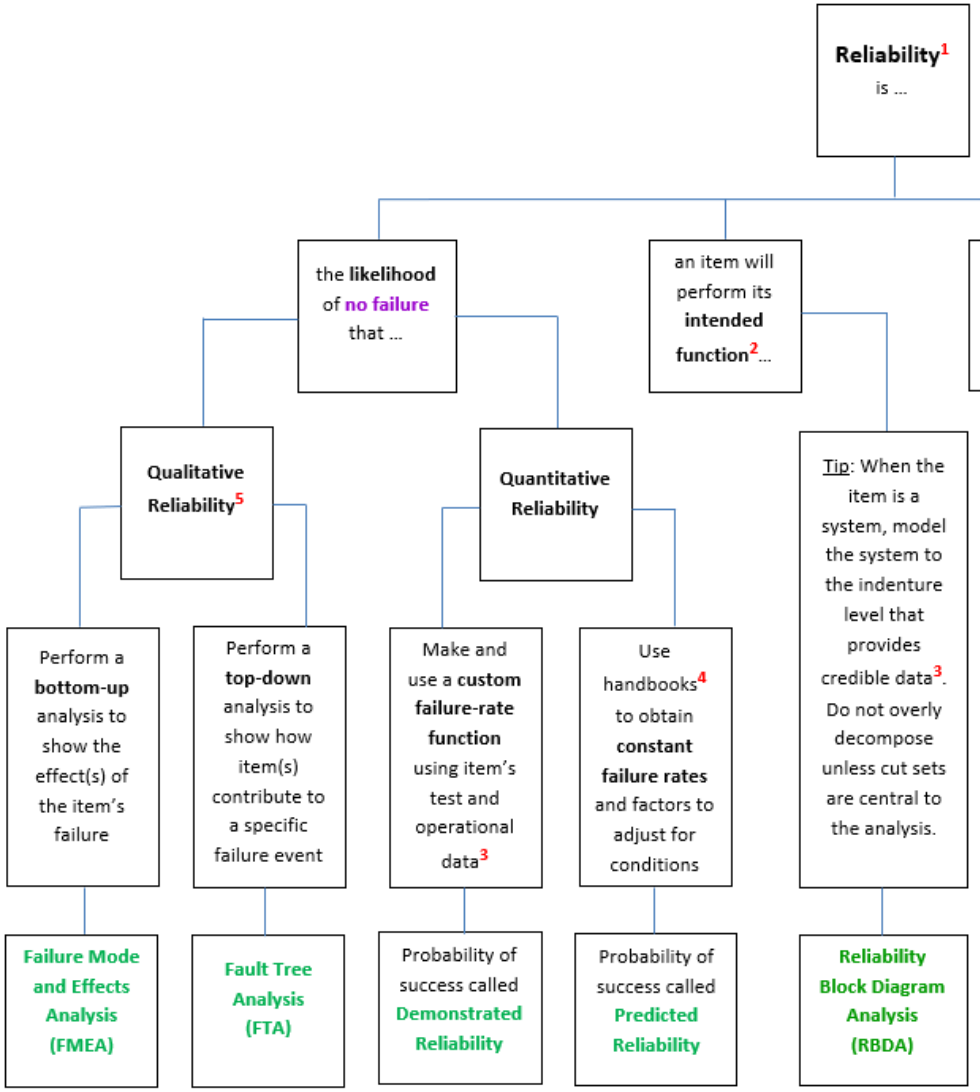
- Example: What should be the top-level goal for the loss of electrical power?

IF		THEN			
Probability electric power is …		Expected electric power unavailability in one year is …			
On	Off	Seconds	Minutes	Hours	Days
0	1	31,536,000.00	525,600.00	8,760.00	365.00
0.9	0.1	3,153,600.00	52,560.00	876.00	36.50
0.99	0.01	315,360.00	5,256.00	87.60	3.65
0.999	0.001	31,536.00	525.60	8.76	0.37
0.9999	0.0001	3,153.60	52.56	0.88	0.04
0.99999	0.00001	315.36	5.26	0.09	0.00
0.999999	0.000001	31.54	0.53	0.01	0.00
0.9999999	0.0000001	3.15	0.05	0.00	0.00

Note: 1 per 1,000,000 is about 1/16 inch per one mile. Actually, 10^6 * 1/16” = 98.64% of 1 mile.

- For sub-goals, start with and decompose the probability portion of the overall goal.
  - This decomposition (called allocation) distributes system level reliability to lower elements.
  - One **allocation method** is the nth root of system reliability; n is the number of serial elements.
- The “nth root” allocation method provides **minimum element reliability** …
  - That can serve as a minimum "design to" requirement for each serial element.
  - Is larger than "**absolute minimum element reliability**," the notion where other serial elements have perfect reliability. Thus, absolute minimum element reliability equals system reliability.

Reliability: From Definition to Analytical Products



1 – For repairable items, Reliability (**R**) is the likelihood an item will remain in an uptime state. Whereas Maintainability (**M**) is the likelihood a **failed item** (an item in a downtime state) will be returned to an uptime state within a given period of time. Availability (**A**) is the likelihood a **repairable item** will be in an uptime state and will recover from downtime states.

2 – Tip: A description of intended function includes the boundaries of the item and the definitions of success and failure.

3 – Data used to model **RMA**:

- Time to failure (TTF)
- Time with no failure (censored, suspended)
- Time to repair (TTR)
- Stress-Strength (Load-Capacity) Interference. This data type models failures caused by variation.

4 – Tip: MIL-HDBK-217 Reliability Prediction of Electronic Equipment is a *controversial source* for data to predict reliability.

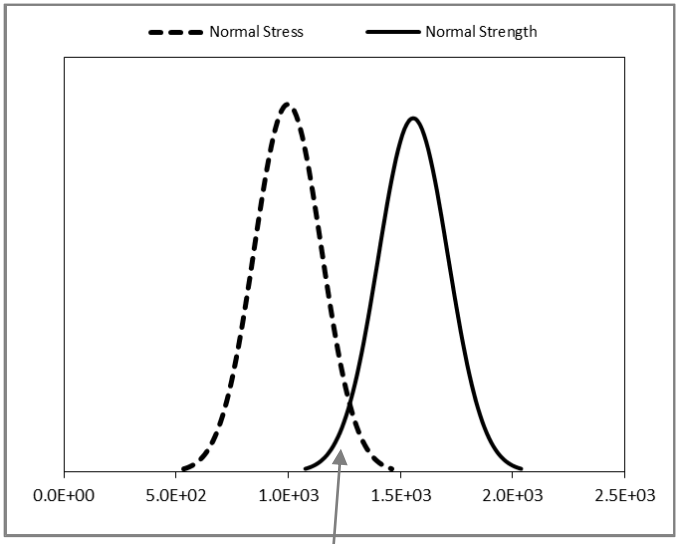
5 – Other analysis techniques include **Sneak Circuit**, **Durability**, **Thermal**, **Humidity**, **Vibration**, **Shock**, **Electromigration**, and **Electromagnetic**.

For a "nay" See slide 11

Required Resources via Statistics: Data and Models

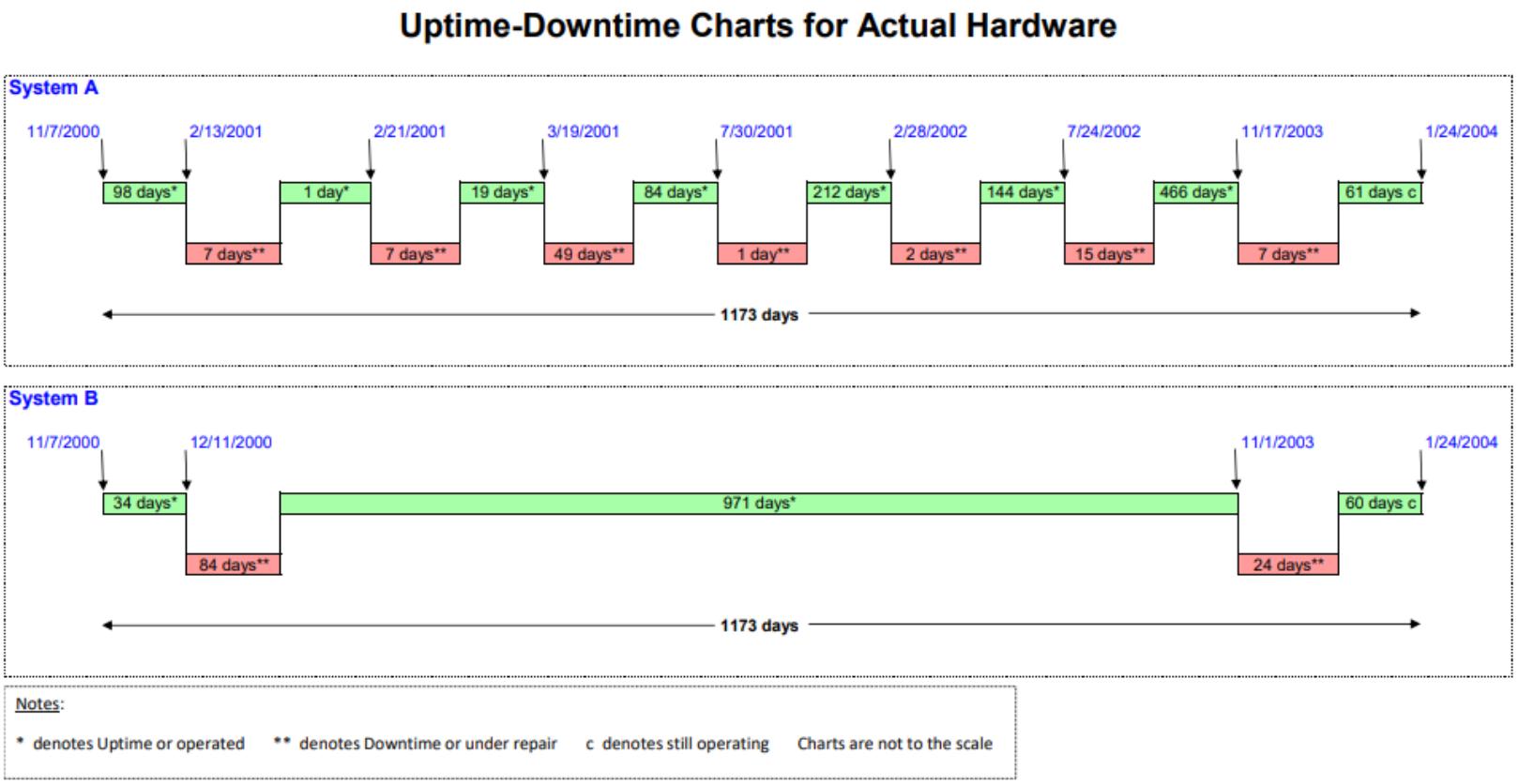
- For the item under study, data includes: (1) Both failures and non-failures (censored data) and (2) Applicable areas: hardware, software, orgware (humans), and interfaces.
- Data types for RMA (more on slide 12) and common (not the only) math models:

1. Time-based (clock) data
   - Continuous (e.g., jet engine run hours)
   - Lifetime math model: Weibull
   - Repair time math model: Lognormal
2. Event-based (demand) data
   - Discrete (e.g., landing gear actuations)
   - Math models: Binomial and Poisson
3. Stress (load) and strength (capacity) data
   - Example: See diagram
   - Note: A **safety factor** does not characterize the uncertainty in the item's stress and strength.
4. Combination
   - Time-to-failure data at different stress levels
   - Common math model: Covariate Weibull



This area corresponds to the **probability of failure** due to variation (uncertainty) in stress and strength.

Example: Time-Based Data for both R and M



MIL-HDBK-217: Should this Data Still Be Used?

MIL-HDBK-217 = Reliability Prediction of Electronic Equipment; Version F = 1991 - 1995

- MIL-HDBK-217 is a reliability prediction methodology for electronic components and devices that is known to be fundamentally flawed in many ways.
- Like their predecessor [MIL-HDBK-217], SAE Reliability Prediction, Bellcore/Telcordia, PRISM, and RIAC 217Plus failed to acknowledge that the degradation and failure of a component cannot be condensed into a single unique "constant failure rate" metric.
- Therefore, we conclude that the MIL-HDBK-217 approach provides the user with values that are inaccurate and misleading.
- The continued use of MIL-HDBK-217 or one of its adaptations can be destructive because it promotes poor engineering practices while also harming the growth of reliability of electronic products.
- DoD should strive for a policy whereby every major subsystem and critical component used in a defense system have *physics-of-failure models [PoF] for component reliability that have been validated by the manufacturer.

* **PoF** is how it should perform under specified conditions. Where as, **statistical modeling** is how it did perform.

Source:

- Reliability Growth: Enhancing Defense System Reliability, National Academy of Sciences, 2015, (pages 238 - 240) from …
- Appendix D, Anto Peter, Diganta Das, and Michael Pecht with the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland.

Definitions: Failure and Failure Data as a Storyline

- For a photocopier, which events are a failure? It depends on the mission and your "model of the world."

• Is old but works	• Has cracked glass	• Is out of toner	• Is in use by others
• Does not do color	• Will not power up	• Is being repaired	• Is not permitted for

- "To understand system assurance, one has to understand the definition of a failure and hazard. If a system does not meet the reasonable expectation of the user, then it has failed, even though it meets the specifications. When failures result in hazards, accidents can occur."

  Source: Assurance Technologies Principles and Practices, 2nd ed., Raheja & Allocco 2006, p. 5

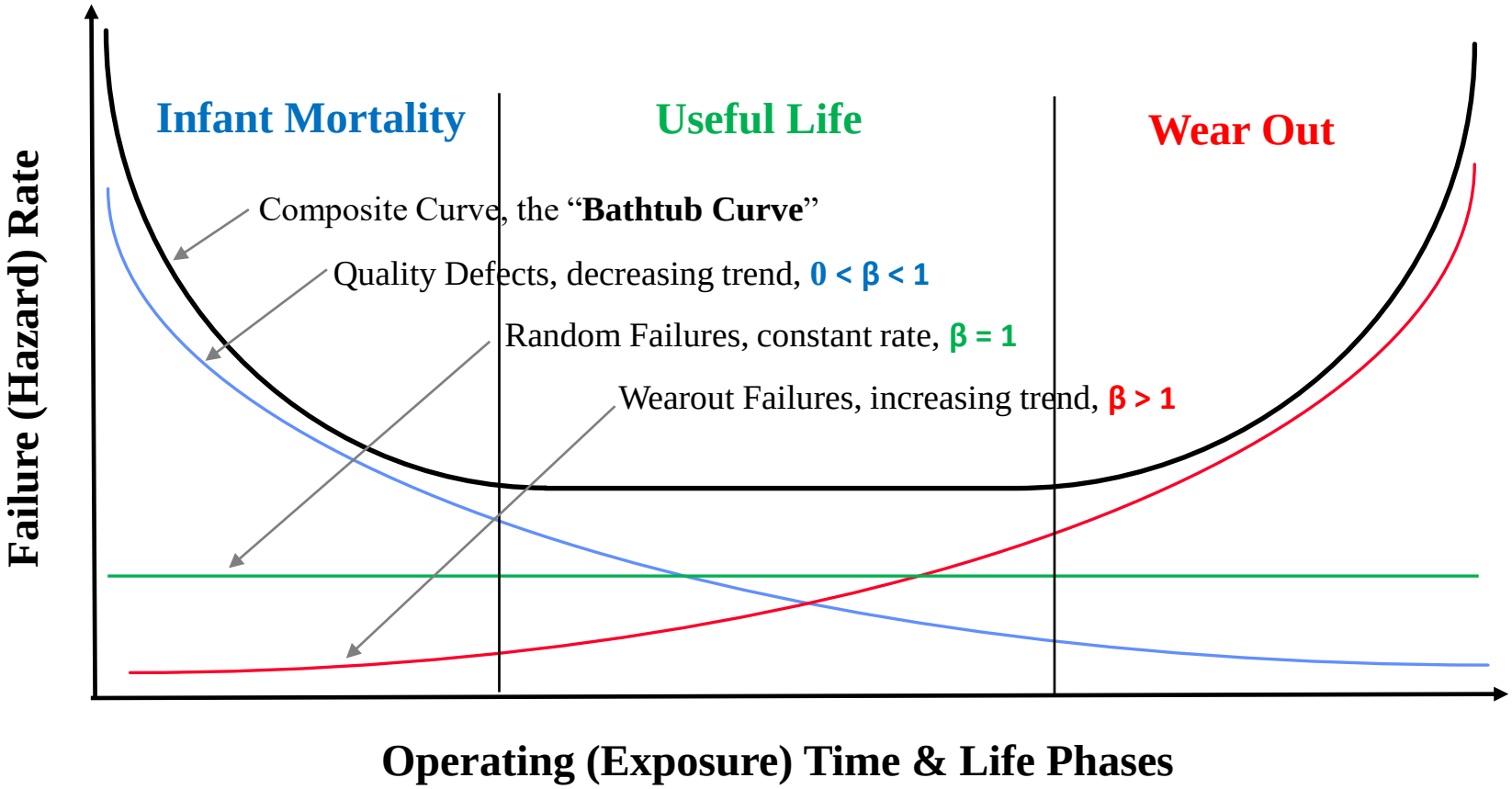
- Vocabulary: Electropedia (IEV Online), a resource from IEC, prepares and publishes international standards.

Term	IEV ref	Definition
• Failure of an item	192-03-01	Loss of ability to perform as required. Also, see 192-03-03
• Hazard	903-01-02	Potential source of harm … qualified with origin (e.g., fire hazard).

- Related Concepts: **Item** = hardware, software, orgware (humans), interfaces, or combination. **Safety** = freedom from accident and loss. **Risk** (in failure space) = potential loss. **RMA** = defined on slides 4 and 5.
- Data Storyline: Failure Event (item's what, when, & where) → Failure Mode (observed what & how much) → Failure Mechanism (why did it fail; causes) → Failure Reoccurrence Control (how to prevent, mitigate, respond to).

Tip: For RMA data, at least collect the operational type. **Operational data**: Operating behaviors and outcomes, inferred by the design model, non-physical characteristics, and uses time and counts. Where as, **Technical data**: Functional capability, contained in the design model, physical characteristics, and uses various units of measure.

Definitions: Bathtub Curve and Failure Rate Types

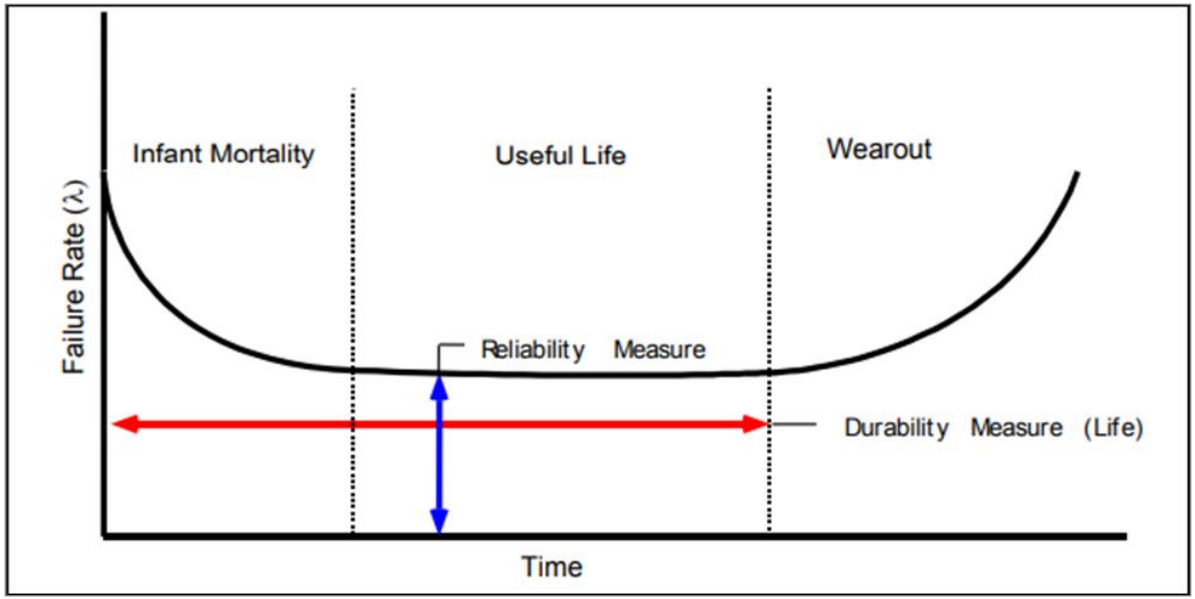


The **Bathtub Curve**, a notional concept, combines three types of failure (hazard) rate functions, λ(t), over an item's life. Included is the Weibull probability distribution's shape parameter (β) for each failure trend type.

Definition: Durability

- "**Durability** is usually defined by the length of a failure free or maintenance free operational period. The basic assumption is that all failures are caused by applied mechanical/thermal stresses, and that there are no failures before the end of the failure free period (useful life) is reached." **Failure rate** (λ) is the height during durability.

Source: System Reliability Toolkit-V, 2015, p. 575



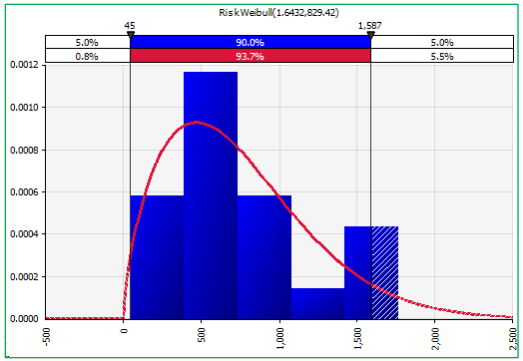
Over the item's entire life, the "**Reliability Measure**" is a function or functions of time, t. Denoted $\lambda(t)$ or h(t).

When the value of $\lambda(t)$ is a constant (c), the expression is commonly written as $\boldsymbol{\lambda = c}$.

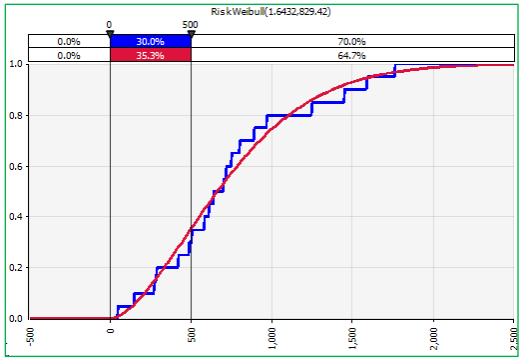
For example, $\boldsymbol{\lambda = 0.001}$ **f/h** means 1 failure every 1000 hours, a rate that remains the same over the item's lifetime or specific to the "Useful Life" phase.

Example: Estimate Reliability Given TTF Data

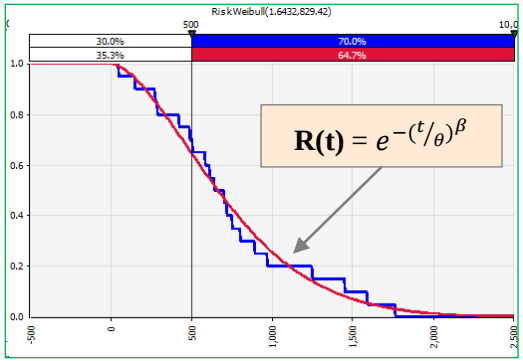
- Question: As a point estimate (not interval estimate), what is the probability item X when new will perform its intended function under stated conditions for a mission time ($\mathbf{t_m}$) equal to 500 hours? Denoted as: $p_S = R(t_m) = Pr[T > t_m] = ?$
- Given: The **time-to-failure** (TTF) data for 20 identical items on test under the stated conditions: 716, 1451, 425, 1763, 1249, 283, 801, 752, 149, 585, 697, 968, 611, 510, 1587, 489, 641, 274, 893, and 45. Note: The mean or average is 744.45 hours. Tip: When applicable, include the time for items that have not failed (censored data).
- Work Process: data → histogram → postulate model and select estimation method → probability density function, **f(t)** → cumulative distribution function, **F(t)** = ∫ f(t) dt for [0, ∞] → 1 – F(t) = **R(t)**, the Reliability model → Use R(t) where t = t_m → $R(t_m)$ = probability of success ($\mathbf{p_S}$).
- Answer: Using the two-parameter Weibull probability distribution as the math model and the Maximum Likelihood Estimation (MLE) method, the model's shape parameter (β) ≈ 1.6432 and scale parameter (θ) ≈ 829.42 hours. Thus, for this math model based on actual data, when mission time = 500 hours, reliability ≈ 0.6470.
- Report: Under the same build and operating conditions, item X has a 64.7% chance in performing its intended function for more than 500 hours; 35.3% chance in not performing its intended function for 500 hours or less. Denoted as: $p_F = F(t_m) = Pr[T \leq t_m] \approx 35.3\%$.



Histogram and the selected Probability Density Function (PDF), **f(t)**



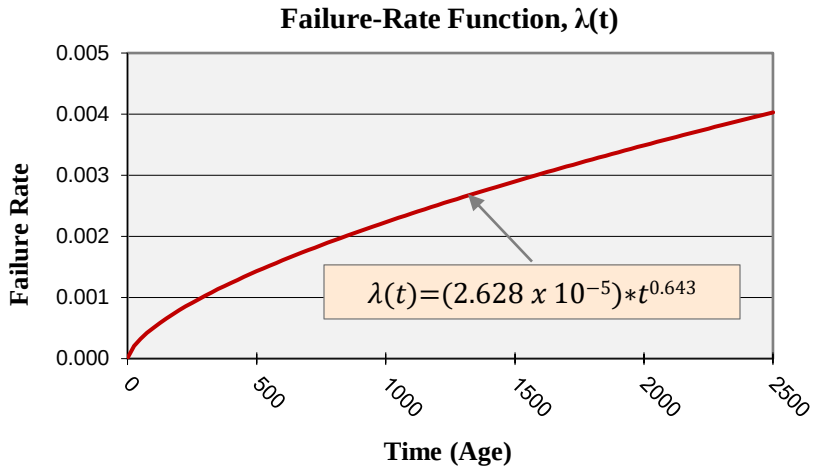
Cumulative Distribution Function (CDF), **F(t)**

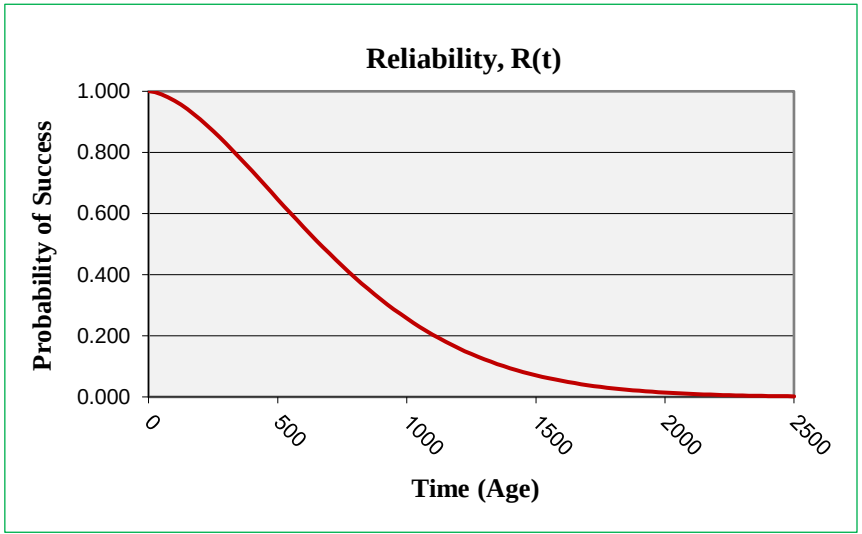


Reliability Function, **R(t)** = 1 – F(t)

Example: Estimate Reliability Given λ(t) Function

- Question: As a point estimate (not interval estimate), what is the probability item X when new will perform its intended function under stated conditions for a mission time ($\mathbf{t_m}$) equal to 500 hours?
- Given: $\boldsymbol{\lambda(t) = (2.628\ x\ 10^{-5}) * t^{0.643}}$, **failure-rate function** (or hazard function) for item X from the lab, a handbook, or journal paper. Note: Confirm before using λ(t) as a model for degradation over time.
- Work Process: Use $\boldsymbol{R(t_1, t_2) = Exp\left[-\int_{t_1}^{t_2} \lambda(x)dx\right]}$ where $\mathbf{t_1}$ = age and $\mathbf{t_2}$ = age + mission time = $t_1 + t_m$. Since item X is new when used, then $t_1 = 0$ which makes $t_2 = 0 + 500$ hours.
- Answer: After integrating λ(t) using the limits [0, 500], $\boldsymbol{R(0, 500) = e^{-0.4353}} \approx 0.6471$.
- Report: Under the same conditions (e.g., build and operate), a new item X has a 64.7% chance in performing its intended function for more than 500 hours; 35.3% chance in not performing its mission for 500 hours or less.





Alternatives to TTF and λ(t): Estimate Reliability

- When these resources cannot be provided for the item of interest …
  - Time-to-failure data (TTF) from test and/or operation (includes non-failures)
  - Failure-rate function λ(t) or the hazard function h(t), then …
- Other options are:
  - *Physics of Failure (PoF), the science and not the math of Reliability
    - NASA Methodology for Physics of Failure-Based Reliability Assessments Handbook
    - Mechanical parts & assemblies (US Navy's Mechrel)
    - Electronic parts and assemblies (Univ of Maryland's SARA)
  - Failure-rate handbooks
    - Quanterion Databooks [NASA internal link]
    - Others: For example, FIDES and MIL-HDBK-217 [not recommended – slide 11]
  - Expert opinion

* **PoF** is how it should perform under specified conditions. **Statistical modeling** is how it did perform.

Examples: Physics of Failure (PoF)

From Design for Reliability, Crowe & Feinberg, 2001

Temperature and Humidity Related Failures - Peck Model

$$A_T = Exp\left\{\frac{E_a}{K_B}\left[\frac{1}{T_{Use}} - \frac{1}{T_{Stress}}\right]\right\}$$

$$A_H = \left(\frac{R_{Stress}}{R_{Use}}\right)^m$$

$$A_{TH} = A_T A_H$$

$$Ln(t_f) = C + \frac{E_a}{K_B T} - m\ Ln(R)$$

Notation

A_H	=	humidity acceleration factor
A_T	=	temperature acceleration factor
A_{TH}	=	temperature-humidity acceleration factor
R_{Stress}	=	relative humidity of test
R_{Use}	=	nominal use relative humidity
T_{Stress}	=	test temperature
T_{Use}	=	nominal use temperature
m	=	humidity constant
E_a	=	activation energy
t_f	=	time to fail
C	=	constant

Temperature Related Failures - Arrhenius Model

$$A_T = Exp\left\{\frac{E_a}{K_B}\left[\frac{1}{T_{Use}} - \frac{1}{T_{Stress}}\right]\right\}$$

$$Ln(t_f) = C + \frac{E_a}{K_B T}$$

Notation

A_T	=	temperature acceleration factor
T_{Stress}	=	test temperature (°K)
T_{Use}	=	use temperature (°K)
E_a	=	activation energy
K_B	=	8.6173×10^{-5} eV/°K (Boltzmann's constant)
t_f	=	time to failure
C	=	constant

Vibration Related Failures - MIL-STD 810E

$$A_V = \frac{T_{Use}}{T_{Stress}} = \left(\frac{W_{Stress}}{W_{Use}}\right)^{M_b}$$

$$\left(\frac{W_{Stress}}{W_{Use}}\right)^{M_b} = \left(\frac{G_{f_{Stress}}}{G_{f_{Use}}}\right)^{2M_b}$$

$$Ln(t_f) = C - M_b\ Ln(W)$$

Notation

A_V	=	vibration acceleration factor
T_{Stress}	=	vibration duration
T_{Use}	=	vibration duration (nominal)
W	=	random vibration input PSD across the resonance bandwidth (G^2/Hz) W_{Stress} is the PSD test stress and W_{Use} nominal use PSD
G_f	=	resonant G sinusoid vibration level
M_b	=	b/2 where b is the fatigue parameter
t_f	=	time to failure
C	=	constant

Temperature Cyclic Related Failures - Coffin Manson Model

$$A_{TC} = \frac{N_{Use}}{N_{Stress}} = \left(\frac{\Delta T_{Stress}}{\Delta T_{Use}}\right)^K$$

$$Ln(N_f) = C - K\ Ln(\Delta T)$$

Notation

A_{TC}	=	temperature cycle acceleration factor
N_{Stress}	=	number of cycles tested
N_{Use}	=	equivalent number of field cycles
ΔT_{Stress}	=	temperature cycle test range
ΔT_{Use}	=	nominal daily temperature change in the field
K	=	temperature cycle exponent
N_f	=	number of cycles to failure
C	=	constant

Wearout (Fatigue) Failures via Uniform Cyclic Load - S-N Curve

$$N = cS\text{^}(-m)$$

Notation

N	=	median number of cycles to failure
S	=	magnitude of the cyclic stress
c and m	=	constants determined experimentally

Data Analysis

The log-log plot of the stress S and the number of cycles N to failure is called the S–N curve.

The S–N curve indicates the cycles to failure at any cyclic stress value between the ultimate stress and the fatigue limit (endurance limit).

Log S vs. Log N data tend to fall along a straight line. The values for c and m can be obtained from a least squares analysis.

Electromigration Failures - Black equation

$$A_J = \left(\frac{J_{Stress}}{J_{Use}}\right)^n Exp\left\{\frac{E_a}{K_B}\left[\frac{1}{T_{Use}} - \frac{1}{T_{Stress}}\right]\right\}$$

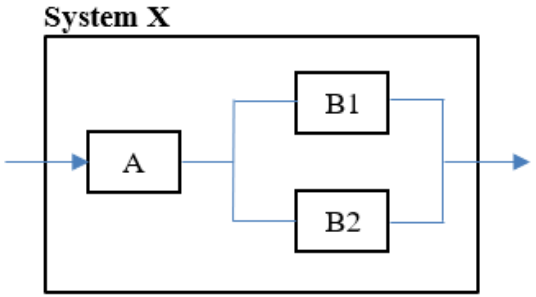
$$Ln(t_f) = C + \frac{E_a}{K_B T} - n Ln(J)$$

Notation

A_J	=	electromigration acceleration factor
T_{Stress}	=	test temperature (°K)
T_{Use}	=	use temperature (°K)
E_a	=	activation energy
K_B	=	8.6173×10^{-5} eV/°K (Boltzmann's constant)
J	=	current density
n	=	current density exponent
t_f	=	time to failure
C	=	constant

Example: Find System Reliability (part 1 of 2)

- **Given**
  - Objective: Find the reliability (probability of success) for System X.
  - Configuration: As shown in the diagram, System X has two items in series; the second item has two items in parallel. All items operate independently of each other.
    - **Independence** means the occurrence of success or failure in any one of the elements does not affect the probabilities of the occurrences of the other events.
  - Selected Probability Laws:
    - Two items in series: Probability of A and B = P(A and B) = P(A)*P(B).
    - Two items in parallel: Probability of B1 or B2 = P(B1 or B2) = 1 - [1 - P(B1)]*[1 - P(B2)].

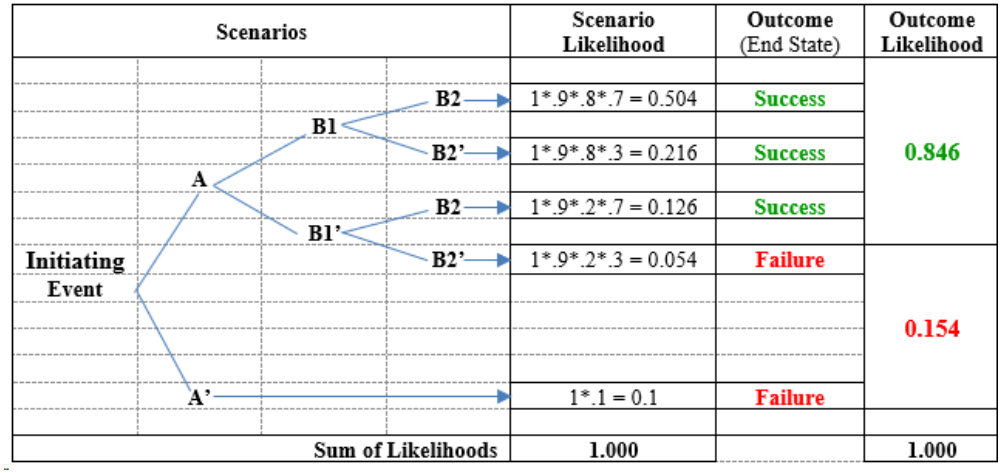


Element	Reliability
A	90%
B1	80%
B2	70%

  - Data (*3 types*): (1) The *reliability for each element* (block). (2) The likelihood System X will be needed, the *initiating event*, is one. (3) The *consequence* (e.g., loss of life, loss of property, additional cost, delayed schedule, loss of reputation) for failure is quantitatively unknown.

Example: Find System Reliability (part 2 of 2)

- **Solution**
  - Write Outcome Statement (in English): Let S denote success and S' denote failure for "not S" or the complement of success. Based on the configuration of System X, system reliability is P(S) = P[A and (B1 or B2)].
  - Method 1 - Solve via Event Tree: (1) A, B1, and B2 generate eight (2^3) possible scenarios. Scenarios need to be assessed for applicability. (2) B is dependent on A. When A fails, then P(A') and P(B given A') = P(A')*P(B given A') = 0.1*0 = 0. (3) B1 and B2 are independent, then P(B1 and B2) = P(B1)*P(B2).



Scenarios	Scenario Likelihood	Outcome (End State)	Outcome Likelihood
A → B1 → B2	1*.9*.8*.7 = 0.504	Success	0.846
A → B1 → B2'	1*.9*.8*.3 = 0.216	Success	
A → B1' → B2	1*.9*.2*.7 = 0.126	Success	
A → B1' → B2'	1*.9*.2*.3 = 0.054	Failure	0.154
A'	1*.1 = 0.1	Failure	
Sum of Likelihoods	1.000		1.000

  - Method 2 - Solve via Probability Formulas:

    P(System X success): From English P(S) = P[A and (B1 or B2)] to Mathematics P(A)*[1-(1-P(B1)*(1-P(B2)] = (0.9)*[1-(1-0.8)*(1-0.7)] = (0.9)*[1-(0.2)*(0.3)] = (0.9)*[0.94] = **0.846**.

    P(System X failure) = 1-P(System X success) = 1-0.846 = **0.154**. Another method is P[(A and B1' and B2') or (A')] = (0.9*0.2*0.3) + (.1) = 0.054 + 0.1 = 0.154.

  - Extra - Quantitative Risk (as an alternative to a risk matrix):

    System X expected risk = P(System X failure)*(System X failure consequence) = (0.154)*Consequence.

Reliability in Relation to Other Crafts

- Reliability is a subset of Quality as per David Garvin's model (go to slide)
- However, Reliability Data is not a subset of Quality Data (go to slide)
- Reliability is not Lean Six Sigma, SPC, Safety, Risk … (go to slide)
- Reliability and Safety are a subset of Risk, and Risk is a subset of Risk-Informed Decision Making (go to slide)
- An Idealized Work Process for Engineering Assurance to produce Safety and RMA Analyses and Assessments (go to slide)

Business Model: "Eight Dimensions of Quality"

- This model by David A. Garvin (Harvard Business School) "breaks down the word quality into manageable parts … can serve as a framework for strategic analysis."

Observe:
3 of the 8 dimensions of pertain to RMA

1. **Performance**: Individual aspects of performance that can usually be ranked objectively.
2. **Features**: Characteristics that enhance the appeal of the item to the user.
3. **Reliability**: A key element for users who need the product to work without failure.
4. **Conformance**: Made exactly as the designer intended; exactly meets customer requirements.
5. **Durability**: Length of a product's life; amount of use before the item deteriorates.
6. **Serviceability** [Maintainability]: Speed with which the product can be put into service when it breaks down. Includes competence and the behavior of the service personnel.
7. **Aesthetics**: How the item looks, feels, sounds, tastes, or smells -- clearly a matter of personal judgement and a reflection of individual preference.
8. **Perceived Quality**: Reputation based on indirect measures inferred from tangible and intangible aspects of the item. Quality is inferred from images, advertising, and brand names rather than reality.

Source: "Competing on the Eight Dimensions of Quality," Harvard Business Review, Nov 1987

Data Types: Quality vs. Reliability

- "Every product possesses a number of elements that jointly describe what the user or consumer thinks of as quality. These parameters are often called **quality characteristics** … several types:
  1. Physical: Length, weight, voltage, viscosity
  2. Sensory: Taste, appearance, color
  3. Time Orientation: Reliability, durability, and serviceability [Maintainability]."

  These three are included in David A. Garvin's "Eight Dimensions of Quality" model

  Source: Introduction To Statistical Quality Control 3rd ed., Montgomery, 1997, p. 6

- "Not all discrepancies or defects lead to low reliability. For example, these defects may degrade quality but not reliability:
  - The wrong shade of a color, a light dent on the surface of a casting, a scratch on the paint, a poor surface finish, the wrong plating on screws

  However, for example, these defects or flaws usually reduce reliability:
  - A poor weld, a cold-soldered joint, leaving out a lock washer, using the wrong flux, not cleaning the surfaces to be joined, a large dent on a spring, an improper crimp on a wire joint."

  Source: Assurance Technologies Principles and Practices, 2nd ed., Raheja & Allocco, 2006, p. 66

Reliability is not …

- Reliability is not …
  - **Lean Six Sigma**.
    - Lean Six Sigma is a process improvement approach that uses a collaborative team effort.
    - Lean Six Sigma is based on DMAIC (define, measure, analyze, improve, and control).
    - Reliability is a "design to" attribute and a measure of effectiveness (not efficiency).
  - **Quality** or **Statistical Process Control** (SPC).
    - "… reliability incorporates the passage of time [number of demands or load], whereas quality does not, because it is a static descriptor of an item … High reliability implies high quality, but the converse is not necessarily true."

      Source: Reliability, Probabilistic Models and Statistical Methods, 3rd ed., Leemis, 2025, p. 4
    - In the Apollo Space Program, quality meant the item was built so that it would work; reliability meant the item was designed so that it would work. Click here for paper.
  - **Safety**.
    - Reliability is concerned with the cause of and likelihood of failure—and ensuring no loss of the item's intended function and mission. Safety is concerned with failures that create hazards.
  - **Risk**.
    - However, "not reliable" (Y) and "not safe" (Z) provide the content for the risk scenario (X).
    - For details on risk as { X, Y, Z }, see Kaplan & Garrick, Jan 1981. More on risk – slide 3.

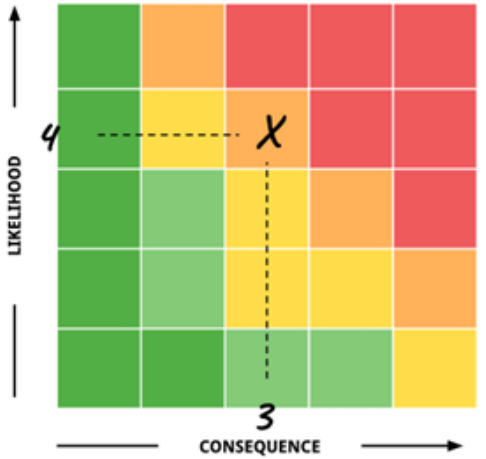
Summary: (Reliability * Safety) ⊂ Risk ⊂ Good Decision

"And" "subset of"

- To communicate both the likelihood and consequence dimensions of risk:
  - The ***not reliable** measure combined with the **not safe** measure …
  - Make and report relative risk as a product (measure) or a cell in a risk matrix (graphic).
  - In failure space, **risk** is potential loss.
- Understanding and prioritizing risk helps to make risk-informed decisions.
- *Various ways to say and determine "not reliable"
  - Probability of failure, denoted p_f.
  - p_f = Unreliability = 1 – Reliability.
  - Reliability Analysis + Fault Tree Analysis = 1.
  - Failure rate (λ) is not a failure probability (p_f).

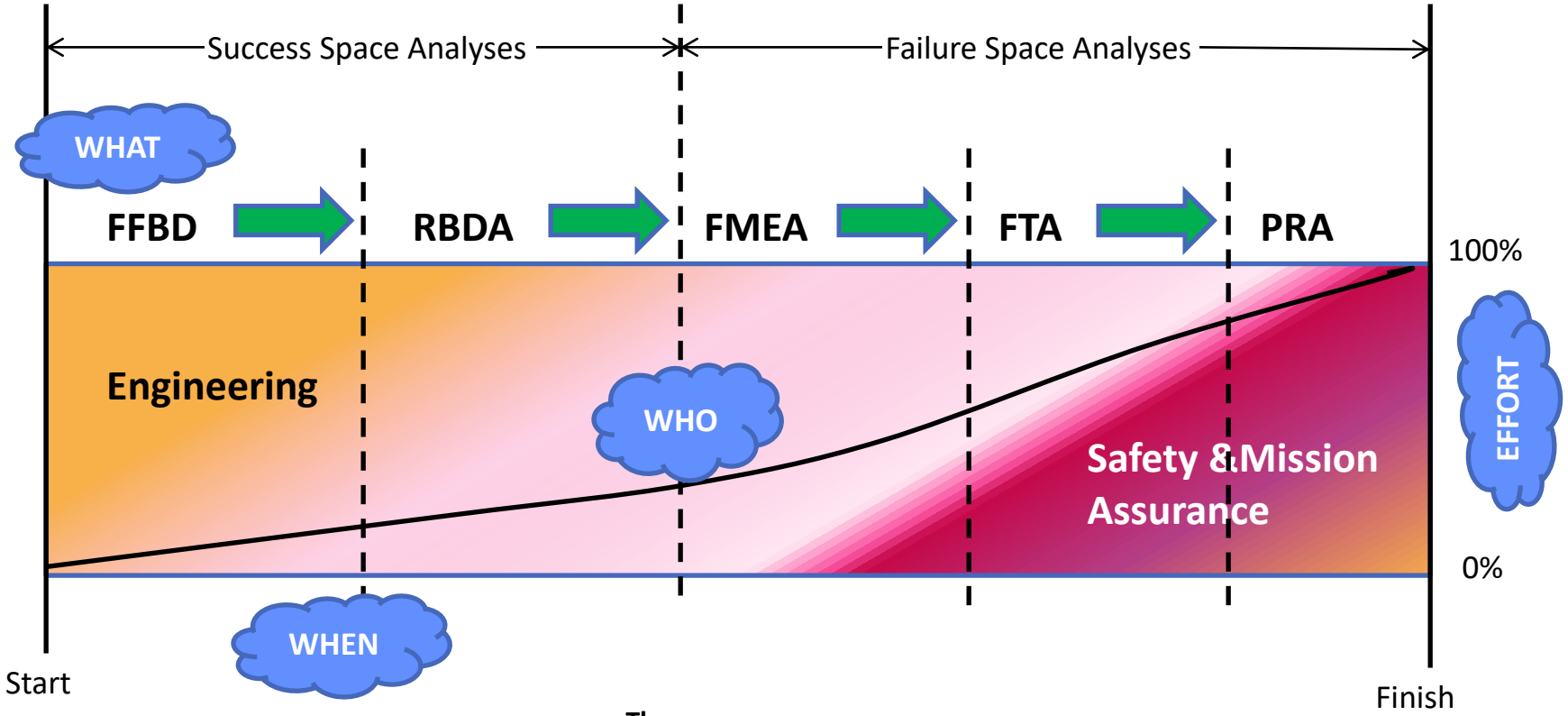
Components of Reliability

American Society for Quality's writeup: What is Reliability?



An Idealized Work Process:

To Produce Safety and RMA Analyses and Assessments



Analytical Products:

FFBD = Functional Flow Block Diagram
RBDA = Reliability Block Diagram Analysis
FMEA = Failure Modes & Effects Analysis
FTA = Fault Tree Analysis
PRA = Probabilistic Risk Assessment

Theme:

This work sequence (WHEN) builds and uses analytical products (WHAT) in an optimum manner—especially during the Design Phase. The appropriate mix of experts (WHO and EFFORT) make and deliver the right analytical product at the right time. In addition to serving the intended purpose at the desired time, each analytical product serves as an input that expands the technical fidelity of the analytical products that follow.

Author:

- Tim Adams is a NASA Senior Engineer in the Engineering Directorate at the Kennedy Space Center (KSC). He serves as a technical resource in engineering assurance with a specialty in quantitative Reliability Engineering and Technical Risk -- and he is the founder and Technical Editor of KSC Reliability, a website for practitioners in Reliability, Safety, and Systems Engineering. Tim started with NASA at the Johnson Space Center with the Mission Operations Directorate. In Reliability and Risk, Tim has received three NASA medals, Employee of the Year Award with Office of the Chief Engineer, Commendation Award in Project Management, and the Silver Snoopy Award from Astronaut William F. Readdy.
- With the American Society for Quality (ASQ), Tim is a senior member, a Certified Reliability Engineer (CRE), and served on the national ASQ team that reviewed the CRE exam. In Mathematics, Tim is a member of Pi Mu Epsilon, a national honorary in Mathematics.

Acknowledgments:

- The Office of Safety and Mission Assurance (OSMA)
  - Brent Heard
  - Anthony "Tony" DiVenti
- Goddard Space Flight Center
  - Charlie Knapp
- Kennedy Space Center
  - Susan Riccetti
  - Anthony "Tony" Mansk