- Decisions Under Risk -

Presented by

Tim C. Adams, ASQ CRE
NASA Kennedy Space Center

October 30, 2003

Outline

Concept

What Is Your Education Background?

- **Determinism:**
  - The doctrine that every event, act, and decision is the inevitable consequence of antecedents (past events) that are independent of the human will.

- **Probabilism:**
  - The doctrine that probability is adequate basis for belief and action, since certainty in knowledge cannot be attained.

Comparing Concepts

	X: Scenario	Y: Likelihood	Z: Consequence
Risk	What can go wrong?	How likely is this to happen?	If it does happen, what are the consequences?
Reliability	Uses historical failure data	Historical failure data is mathematically modeled to predict failures	The element under study either does or does not meet the failure definition
Safety	Relies heavily on the identification of hazards	Likelihood is based on judgment and a qualitative scale	Evaluates hazardous states that could occur from both correct and incorrect element behavior

Concept

What is Reliability?

- **Reliability** is defined as
  - *the probability that an item will perform it intended function for a given time period under a given set of conditions.*
- Another name for reliability (R) is the "**probability of success**" (p_s). Many times at NASA, we speak in terms of the "**probability of failure**" (p_f) being unreliability (U).
- Fundamental math rule: $p_s + p_f = 1$ or $R + U = 1$.

Concept

Where does Reliability originate?

- It is design engineering where most of the true reliability work is done.
- Reliability Engineering is not just the statistical treatment of failure data.
- True reliability is built into the design and is called **inherent reliability**.
- Attempts to improve inherent reliability after design through manufacturing, testing, and preventive maintenance are usually expensive and inefficient. Thus, the system/product's inherent reliability is generally viewed as the system/product's highest reliability.
- Reliability requirements are an integral part of engineering specifications. As the formal definition implies, at least four items must be contained in a **reliability requirement** or specification, namely:
  - The intended function (mission) to be performed.
  - The desired mission time.
  - The operating environment.
  - The probability of success or no failure that the product will perform its intended function.

Product

Reliability made them money

- "Procter & Gamble borrowed reliability engineering from Los Alamos to boost output and save $1 billion."
- "When P&G began reliability in the 1980s…[they] were building lousy systems and just figuring out how to fix them faster and faster." **
- P&G now sells its "reliability toolbox" to other companies.

** **Reliability** deals with reducing the frequency of breakdowns. **Maintainability** deals with reducing the duration of breakdowns or downtime. **Availability** is a function of Reliability and Maintainability; i.e., A = uptime/(uptime + downtime).

Ref: "Using Rocket Science to Make Sugar Drinks," Fortune, November 26, 2001

Product

Reliability helped them to make decisions

1. A recent system failure caused major embarrassment as well as much expense. Should this system be replaced with new technology or upgraded? If upgraded, identify the system elements causing the trouble and the required reliability.
2. During a final review of a system prior to shipment, questionable test data on one of the parts appears. Assuming all other parts perform as intended, what is the risk of shipping and advising the customer to use the system anyway? In particular, what is the likelihood the system will not perform to meet minimum requirements?
3. The test director wants to know if testing can stop after receiving no failures in 360 tests on a life-critical item. Does this testing certify that the item is safe?

Product

These were NASA decisions. Details ...

- Case 1: Fuel Cells on the Space Shuttle's Orbiter caused a minimum duration flight (MDF) during STS-83.
  - In addition to the MDF, a previous launch delay and numerous maintenance actions during turnaround made this system an "upgrade" candidate.
  - A detailed reliability and maintenance (R&M) analysis and assessment report on all Fuel Cell line replaceable units (LRU's) from the STS-26 to STS-85 time period was completed.
  - This R&M assessment was instrumental in the decision to change regulator material in all LRU's for $12M instead of replacing with a new design estimated at $50M.
  - This report can be found on JSC SRQA, Code NC's web page at http://wwwsrqa.jsc.nasa.gov/TAL/docs/FuelCell-RM.pdf

Product

These were NASA decisions. Details ... (cont.)

- Case 2: The test data was on the Hall resolvers (sensors) and was generated by the vendor. These sensors are used on the Control Moment Gyros (CMGs), a Space Shuttle payload for Space Station's Flight 3A.
  - A reliability analysis presented at the Space Station Control Board (SSCB) showed that there was a 4-6% chance of not having a minimum CMG. A minimum CMG is at least 1 of 2 sensors working in each gyro and at least 2 of the 4 gyros working for 5, 7, or 9 thermal cycles. This cycle count was used because sensor heaters would not be available on the Station until after that number of thermal cycles occurred.
  - The consequence of not having a minimum CMG meant that 6 metric tons of propellant would have to be consumed at a cost of $100 million.

Product

These were NASA decisions. Details ... (cont.)

- Case 3: During July 2000, White Sands Test Facility (WSTF) conducted 360 tests to determine if ignition would occur during the presence of a small quantity of hydrocarbon oil in 100% oxygen under adiabatic compression, the compression heating of oxygen. None of these WSTF tests produced ignition.
  - This test was in response to a hydrocarbon oil contaminate found in the Primary Life Support System (PLSS) used in Extravehicular Mobility Unit (EMU).
  - The maximum failure rate was determined with a high degree of statistical confidence using classical test statistics. This failure rate did not meet the program's failure-rate goal, and more testing was required if only this analysis method was to be used to make a decision. Two other analysis methods were used.
  - The second method used the Arrhenius Reaction Rate Model. This model adjusted the failure rate found in the first method since all WSTF testing was done under stressed conditions (higher pressure). The failure rate goal was surpassed.
  - The third method compared EMU to similar test data. This method later required combustion Physics (i.e., Semenov equations) to address the heat loss. It was found the reaction rate was not fast enough to cause an ignition in the PLSS.

Why Reliability is Important?

Because Reliability affects:

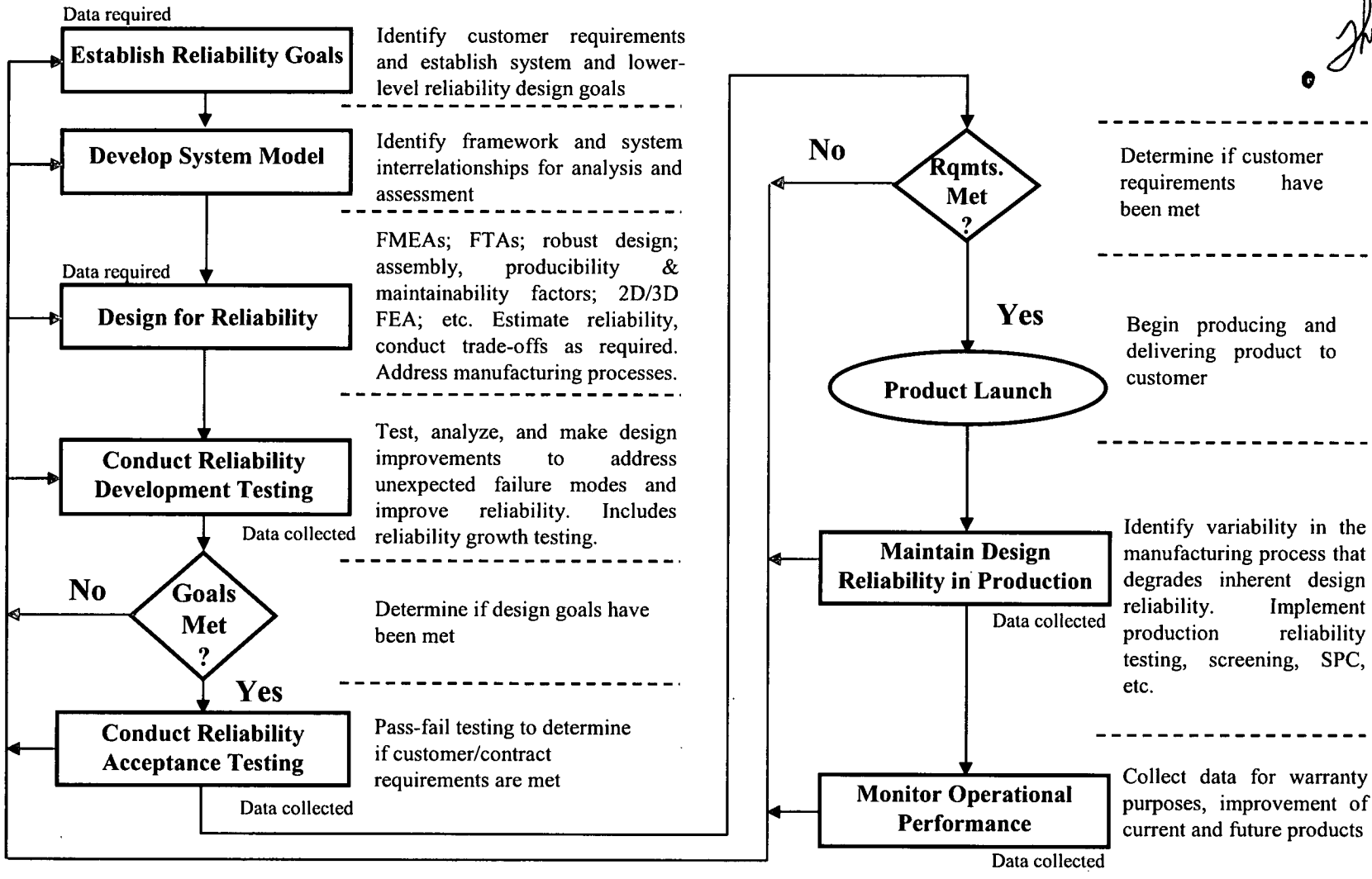
- System/Product safety
- System/Product availability
  - "Inherent Availability" is a function of reliability and maintainability where A = uptime/(uptime + downtime) = MTBF/(MTBF + MTTR).
- Agency/Company risk and liability
- Costs
  - Life cycle costs, costs from inception to disposal
  - Warranty costs
- Customer confidence and future sales (funding)

In summary, Reliability is a prime measure of quality as viewed by the customer

Process

A Comprehensive Reliability Strategy & Program

From the Reliability Analysis Center (RAC)



Note: Data is from the FRACA (PRACA) System.

Process

Design Phase Reliability Tools & Techniques

- To specify reliability: Use all four parts of the reliability definition.
- To prevent failures: Use the *design strategies* in the following order.
  - Improve the design to eliminate the failure mode.
  - Design for fault tolerance (redundancy).
  - Design to be fail-safe (i.e., failure affects function but no injury or additional damage will occur).
  - Provide early warnings of failure through fault diagnosis.
  - Note: If these strategies are not viable, the designer may choose to issue special maintenance instructions and/or use Reliability-centered Maintenance (RCM).
- To improve reliability (part 1): Use the applicable *design strategies*.
  - **Zero Failure Design:** Critical failures are entirely eliminated by design.
  - **Fault Tolerance:** Redundant elements are used to switch over to a backup or alternative mode.
  - **Derating:** A component is used much below its capability rating.
  - **Durability:** A component is designed a have a longer "useful life" or is designed for damage tolerance.
  - **Safety Margins:** Design for all applicable worst-case stresses and environments.

Process

Design Phase Reliability Tools & Techniques (cont.)

- To verify reliability: Use the applicable *analytical tools.*
  - **Design Reviews:** Challenges the design from different viewpoints and identifies and assesses risk (technical, schedule, and cost).
  - **Reliability Allocation, Modeling, And Prediction:** Provides a hierarchy of design requirements along with the distributed reliability goal, a model for system configuration, and estimated (predicated) reliability of the configuration.
  - **Design Failure Mode, Effects, And Criticality Analysis (Design FMECA or FMEA):** Starts at the component level. Asks what can go wrong and how does it affect the system. Is an inductive (bottom up) and systematic method and is mostly qualitative.
  - **Fault Tree Analysis (FTA):** Starts at the system major failure or undesired event and decomposes to it contributing fault occurrences. Is a deductive (top down) and unstructured method; uses symbolic logic and is always qualitative (e.g., identifies cut sets) with the option of being quantitative.
  - **Sneak Circuit Analysis:** Identifies failures not caused by part failures but are caused by logic flaws.
  - **Worst-Case Analysis:** Typically, used on circuits to evaluates performance when components are at their high and low values.
  - **Statistical Analysis:** Uses time-to-failure distributions, pass-fail distributions, and stress-strength distributions to measure predicated or demonstrated reliability.
  - **Quality Function Deployment (QFD):** A method for converting customer needs into engineering requirements.
  - **Robust Design (Design of Experiments, DOE):** Parameters and tolerance ranges are scientifically established to optimize performance so that the item is robust in a variety of conditions.

Process

Design Phase Reliability Tools & Techniques (cont.)

- To improve reliability (part 2): Use the applicable *engineering tests.*
  - **Reliability Growth Tests:** A test that identifies problems and solves them as the design progresses. Thus, is essentially, a "test, analyze, and fix" method that is used in a closed-loop corrective action manner.
  - **Durability Tests** – Typically, **Accelerated Tests** that determine the failure rate for the entire expected life. Duplicates field failures by providing a harsher but representative environment. Performed instead of testing under normal conditions in order to eliminate testing that would otherwise take months or years.
  - **Qualification Tests** – Consist of stressing the product for all expected failure mechanisms. The test can be stopped if there are no failures during the expected life—thus, are performed to measure the achievement of the reliability requirement. Note: **Demonstration Tests** or **Design Approval Tests** are similar and usually require stressing during only a portion of the useful life. See the tests used in the manufacturing phase.

Process

Manufacturing Phase Reliability Tools & Techniques

- To prevent or reduce failures: Use the following *analytical tools*.
  - **Process Failure Mode, Effects, And Criticality Analysis:** Used on the manufacturing process before it is installed. Similar to Design FMECA.
  - **Statistical Process Control:** Designed to ensure that the manufacturing process continues to produce products with no more than expected variation in the critical parameters. Often considered a test for determining the control of quality instead of reliability.
- To prove reliability: Use the applicable *accounting tests*.
  - **Environmental Stress Screening Tests:** Also, known as **Burn-in and Screening Tests**. Tests to catch "infant mortality" failures. If the product is manufactured properly, these tests are not required. Note: These tests are also performed in the Design Phase such that early failures do not mask the true reliability. Unfortunately, these tests are sometimes used as the "final word." As a result, the screening may not be long enough and weak products may be provided to the customer.
  - **Production Reliability Acceptance Tests:** Also, known as **Failure Rate (MTBF) Tests.** Used to detect any degradation in the inherent reliability of a product over the course of production and to assure products being delivered meet the customer's reliability requirements and/or expectations (by testing a production lot and accepting or not accepting based on a sampling plan). Also, used to qualify new products.

Process

User's Phase Reliability Tools & Techniques

- Use the following *strategies* in the User's Phase:
  - **Failure Reporting, Analysis, Corrective Action System:** Provides the data needed to identify deficiencies for correction to ensure that inherent reliability is not degraded. This system is typically used to record data for product failures that occurred during all phases of testing as well as in the field. Also, the data from this system is typically used to detect trends as early as possible and to respond accordingly in a timely and preventive manner.
  - Note: **Weibull Analysis**, a type of statistical analysis, is a good *tool* for identifying trends in non-repairable systems. For repairable systems that are not repaired "good-as-new," use the **Laplace Test**.
  - **Warranties:** An attribute where reliability easily affects the manufacturer's current and future revenues. One of the biggest challenges facing manufacturers is competition due to longer warranties.

Reliability and Its Program
-- Final Comments --

- Reliability is a performance factor determined in design.
- An effective reliability program is integrated into the overall program plan, is proactive, emphasizes finding and eliminating design weaknesses, and must be tailored to the product and program.
- Predictions and assessments are useful but can be misinterpreted and are subject to assumptions.
- Analytical tools help the designer incorporate reliability.
- Testing helps to fill in the gaps of our analyses.
- Data collection and analysis is a key element.