Reliability Program Overview for Developers

Toolbox

Amnon Ganot - October, 2010

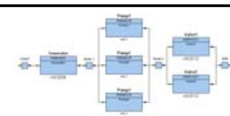
Agenda

- *Metrics*
  - Reliability
  - Failure Rate
  - MTTF / MTBF
  - Expected Life
  - MTTR
  - Availability
  - Reliability Growth
- *Toolbox*
  - Design
  - Tests
  - Monitor
- *Reliability Assurance Plan*
- *summary*

Agenda

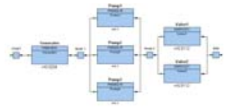
- *Metrics*
  - Reliability
  - Failure Rate
  - MTTF / MTBF
  - Expected Life
  - MTTR
  - Availability
  - Reliability Growth
- *Toolbox*
  - Design
  - Tests
  - Monitor
- *Reliability Assurance Plan*
- *summary*

RBD



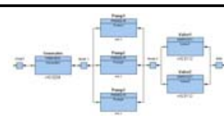
- A *Reliability Block Diagram* (RBD) is used to performs the system reliability, maintainability and availability analysis on large and complex systems using block diagrams to show network relationships

RBD



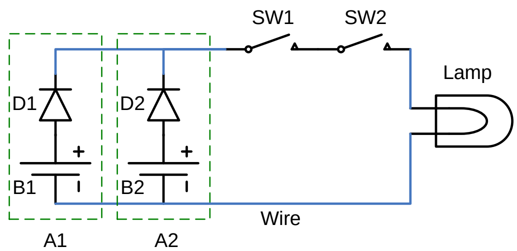
- The structure of the *Reliability Block Diagram* defines the logical interaction of failures within a system that are required to sustain system operation (specific mission or function)

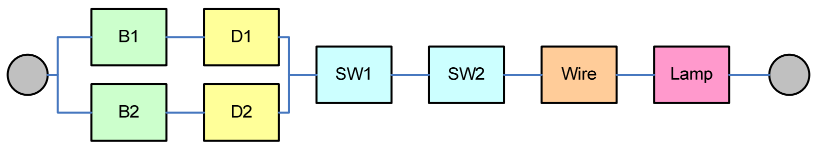
RBD



- A *Reliability Block Diagram* (RBD) is an event diagram
- It answers the following question:
  - Which element of the item under consideration are necessary for the fulfillment of the required function and which can fail without affecting it?
- The elements which are necessary for the required function are connected in *series*, while elements which can fail with no effect on the required function (redundancy) are connected in *parallel*
- **Each required function has its own *Reliability Block Diagram***

RBD - Example

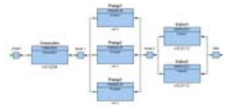




RBD - Data

- Each block represents the relevant unit's failure function. The source for the failure function can be one of the followings:
  - Field Data
  - Test Data (Reliability Lab)
  - Standards (e.g., MIL-HDBK-217, Bellcore, etc.)

RBD - Procedure

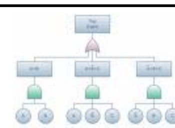


- Define of the required function and its associated mission profile
- Derivation of the corresponding reliability block diagram (RBD)
- Determination of the operating condition of each element of the RBD
- Determination of the reliability function for each element of the RBD
- Elimination of reliability weaknesses and return to the second step, as necessary

Gertron גרטרון בע"מ

Confidential

FTA



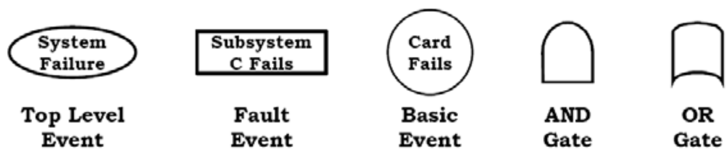
- Fault Tree Analysis (FTA) is a systematic methodology for determining all possible ways that an undesirable event, such as system failure, can occur

Gertron גרטרון בע"מ

Confidential

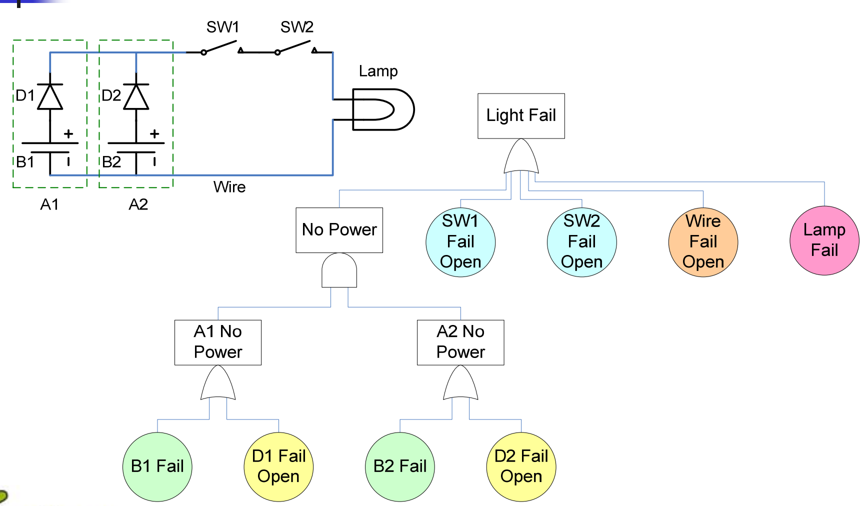
FTA

- An undesirable event is topologically represented with the following symbols:



- An AND gate represents a situation whereby it is TRUE if all incoming elements are TRUE
- An OR gate represents a situation whereby it is TRUE if one or more incoming elements are TRUE
- There are many more symbols types (e.g., Ordered AND gate, Exclusive OR gate, Inhibit gate, Majority gate, etc.)

FTA - Example



FTA

- Strength
  - Extremely useful during initial design phase
  - Can be used to determine system reliability
  - Recent advances with dynamic fault tree has more gate types and therefore more capability
- Weakness
  - When RBDs are large, compounding AND and OR logic structures can be difficult to comprehend (conveys the same information as RBDs but not as visually intuitive)
  - Difficult to model repair and logistics
  - Difficult to model dependencies among components

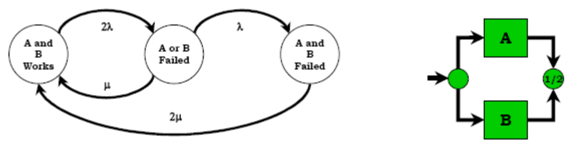
FTA - Data

- Each block represents the relevant unit's failure function. The source for the failure function can be one of the followings:
  - Field Data
  - Test Data (Reliability Lab)
  - Standards (e.g., MIL-HDBK-217, Bellcore, etc.)

Markov Model

- The Markov Modeling technique analyzes systems based on the probability of the system transitioning between various distinct states
- For example a series Markov Model

- And for a *1-out-of-2* redundant system



Markov Model

- Strengths
  - Powerful tool for analyzing small subsystems with complicated internal dependencies
  - Ability to model component dependency issues such as cold or warm standby, maintenance personnel competition, and sparing
  - Great for determining steady state availability
- Weaknesses
  - State space explosion occurs with relatively few components
  - Generally assumes exponential failure and repair rates

Reliability Allocation

- Reliability Allocation deals with the setting of reliability goals for individual subsystems such that a specified system reliability goal is met and the hardware and software subsystem goals are well balanced among themselves
- Well-balanced usually refers to approximate relative equality of development time, difficulty, risk, or to the minimization of overall development cost/time

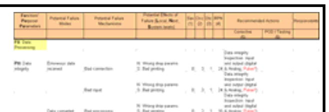
Reliability Allocation

- The most commonly used method to conduct the reliability allocation is the ARINC technique
- The main idea is to allocate failure rates in proportion to the current (known) failure rates
- The ARINC approach, proposed by the Aeronautical Research Inc., assumes that all components are
  - Connected in series
  - Independent of each other
  - Exponentially distributed
  - Have a common mission time

Reliability Prediction

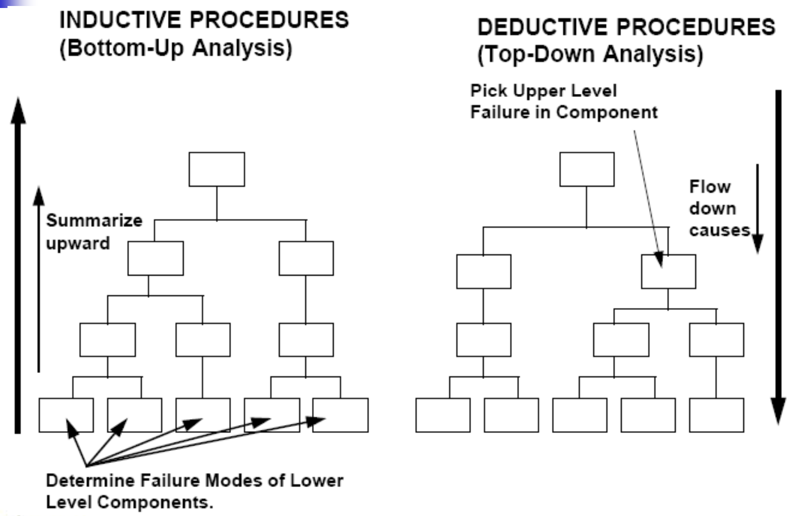
- When actual product reliability data is not available, standards based reliability prediction may be used to evaluate design feasibility, compare design alternatives, identify potential failure areas, trade-off system design factors and track reliability improvement
- Major Reliability Prediction Standards:
  - MIL-HDBK-217F
  - Bellcore/Telcordia
  - NSWC (Mechanical)

FMEA



- Failure Mode & Effect Analysis (FMEA)
- The primary purpose of the *Failure Mode and Effect Analysis* (FMEA) is to collect and evaluate the necessary system design information to identify and eliminate or control all failure modes that pose unacceptable risk

FMEA



FMEA – Types (1)

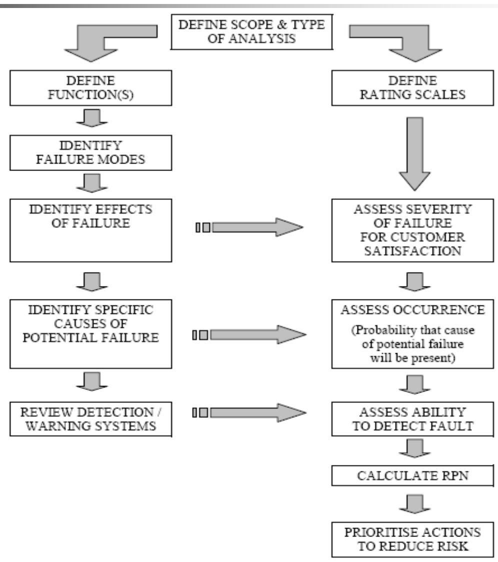
- *Concept FMEA*
  - CFMEA is used to analyze concepts in the early stages before hardware is defined (most often at system and subsystem)
  - It focuses on potential failure modes associated with the proposed functions of a concept proposal
  - This type of FMEA includes the interaction of multiple systems and interaction between the elements of a system at the concept stages
- *Functional FMEA*
  - FFMEA examines the intended functions that a product, process, or service is to perform rather than the characteristics of the specific implementation
  - When a functional FMEA is developed, a functional block diagram is typically used to identify the top-level failures for each block in the diagram

FMEA – Types (2)

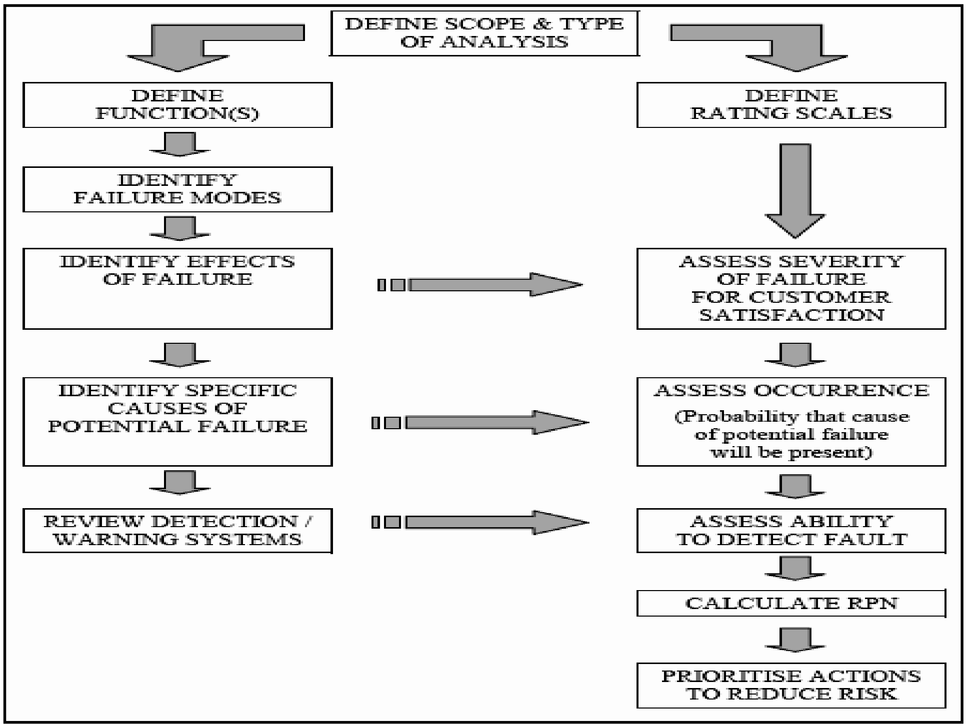
- *Design FMEA*
  - DFMEA is used to analyze product designs before they are released to production. DFMEA focuses on potential failure modes associated with the functions of product and caused by the design deficiencies
- *Process FMEA*
  - PFMEA is used to analyze the already developed or existing processes. PFMEA focuses on potential failure modes associated with both the process safety/effectiveness/efficiency, and the functions of a product caused by the process problems

Gertron
גרטרון בע"מ

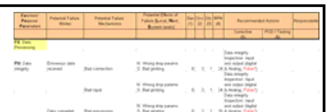
FMEA - Flow



Gertron
גרטרון בע"מ



FMEA - Template

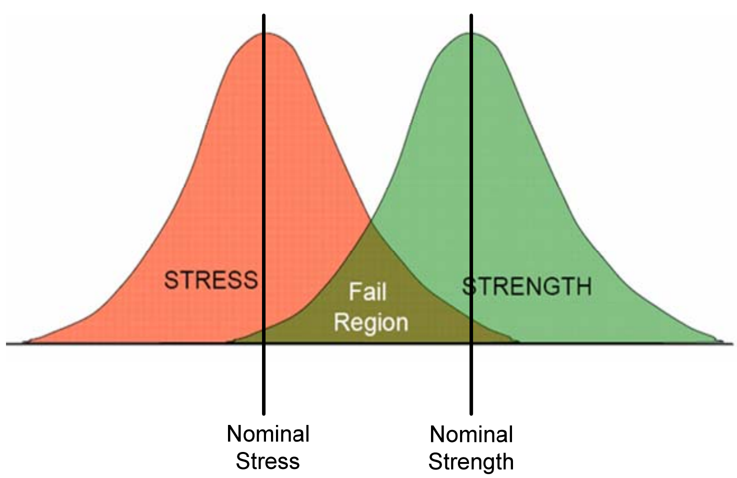


Function/ Purpose/ Parameters	Potential Failure Modes	Potential Failure Mechanisms	Potential Effects of Failure [Local, Next, System levels]	Sev (1)	Occ (2)	Dtc (3)	RPN (4)	Recommended Actions		Responsibility
								Corrective (5)	POD / Testing (6)	
FU: Data Processing										
PU: Data integrity	Erroneous data received	Bad connection	N: Wrong drop params S: Bad printing	8	3	1	24	Data integrity Inspection: Input and output (digital & Analog, Pulse?)		
		Bad input	N: Wrong drop params S: Bad printing	8	3	1	24	Data integrity Inspection: Input and output (digital & Analog, Pulse?)		
	Data corrupted	Bad processing	N: Wrong drop params S: Bad printing	8	2	1	16	Data integrity Inspection: Input and output (digital & Analog, Pulse?)		

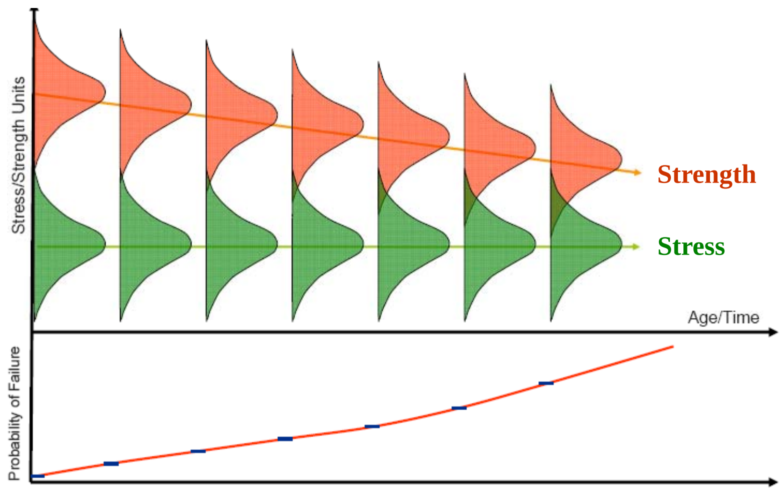
Stress-Strength

- An item fails when the applied stress exceeds the strength of the item
- In general, designers design for a normal strength and a nominal stress that will be applied to an item
- One must also be aware of the variability about the stress and strength nominal's

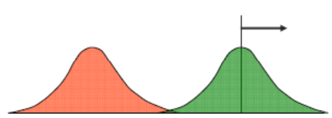
Stress-Strength Analysis



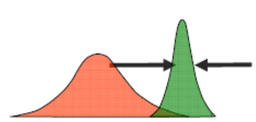
Stress-Strength Vs. Age



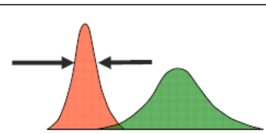
Stress-Strength: Strategy



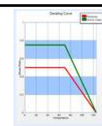
Increase Design Margins



Reduce Variation in Product Strength

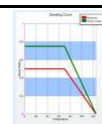


Reduce Effect of Usage/Environment



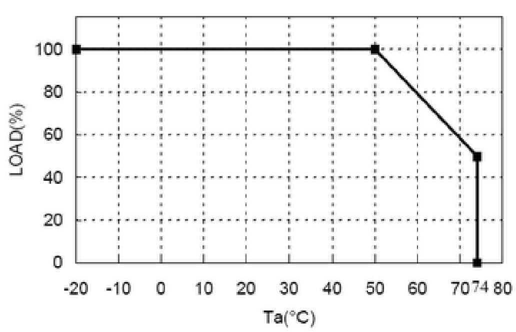
Derating

- The practice of limiting electrical, thermal and mechanical stresses on parts to level below their specified ratings is called derating
- There is a direct proportion between failure rate and stress level, as you lower the stress level (derating), you reduce the device failure rate
- One rule of thumb that is commonly used in electronics is that a 50% derating can decrease the failure rate more than 30%

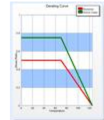


Derating

- The lowering of the rating of an item in one stress field, allows an increase in another stress field

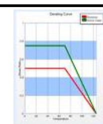


Derating Level



- The following factors influence the required derating level:
  - Reliability Challenge
  - System Repair
  - Safety
  - Size / Weight
  - Life Cycle

Derating Level



Factors		Score
Reliability Challenge	• For *proven design*, achievable with standard parts/circuits	1
	• For high reliability requirements, *special design features* needed	2
	• For new design challenging the state-of-the-art, *new concept*	3
System Repair	• For *easily accessible*, quickly and economically repaired systems	1
	• For high repair cost, limited access, *high skill levels required*, very low downtimes allowable	2
	• For *nonaccessible repair*, or economically unjustifiable repairs	3
Safety	• For *routine safety* program, no expected problems	1
	• For potential system or equipment *high cost* damage	2
	• For potential *jeopardization of life* of personnel	3
Size, Weight	• For no significant design limitation, *standard practices*	1
	• For special *design features* needed, difficult requirements	2
	• For new concepts needed, severe design limitation	3
Life Cycle	• For *economical repairs*, no unusual spare part costs expected	1
	• For potentially *high repair cost* or unique cost spares	2
	• For systems that may require *complete substitution*	3

Instructions: Select score for each factor, sum and determine derating level or parameter.

Derating Level	Total Score
I	11 - 15
II	7 - 10
III	6 or less

Factors		Score
Reliability Challenge	• For *proven design*, achievable with standard parts/circuits	1
	• For high reliability requirements, *special design features* needed	2
	• For new design challenging the state-of-the-art, *new concept*	3
System Repair	• For *easily accessible*, quickly and economically repaired systems	1
	• For high repair cost, limited access, *high skill levels required*, very low downtimes allowable	2
	• For *nonaccessible repair*, or economically unjustifiable repairs	3
Safety	• For *routine safety* program, no expected problems	1
	• For potential system or equipment *high cost* damage	2
	• For potential *jeopardization of life* of personnel	3
Size, Weight	• For no significant design limitation, *standard practices*	1
	• For special *design features* needed, difficult requirements	2
	• For new concepts needed, severe design limitation	3
Life Cycle	• For *economical repairs*, no unusual spare part costs expected	1
	• For potentially *high repair cost* or unique cost spares	2
	• For systems that may require *complete substitution*	3

Instructions: Select score for each factor, sum and determine derating level or parameter.

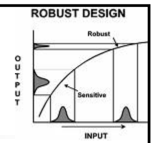
Derating Level	Total Score
I	11 - 15
II	7 - 10
III	6 or less

Gertron
גרטרון בע"מ

Derating Level

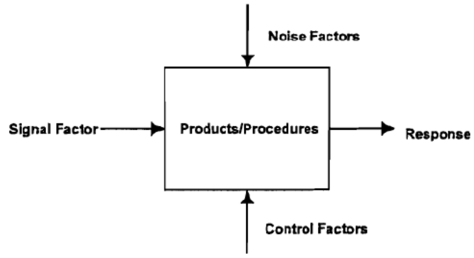
Part Type	Derating Parameter	Derating Level I	II	III
Capacitors				
• Film, Mica, Glass	DC Voltage	50%	60%	60%
	Temp from Max Limit	10°C	10°C	10°C
• Ceramic	DC Voltage	50%	60%	60%
	Temp from Max Limit	10°C	10°C	10°C
• Electrolytic Aluminum	DC Voltage	--	--	80%
	Temp from Max Limit	--	--	20°C
• Electrolytic Tantalum	DC Voltage	50%	60%	60%
	Temp from Max Limit	20°C	20°C	20°C
• Solid Tantalum	DC Voltage	50%	60%	60%
	Max Operating Temp	85°C	85°C	85°C
• Variable Piston	DC Voltage	40%	50%	50%
	Temp from Max Limit	10°C	10°C	10°C
• Variable Ceramic	DC Voltage	30%	50%	50%
	Temp from Max Limit	10°C	10°C	10°C

Gertron
גרטרון בע"מ

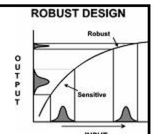


Robust Design

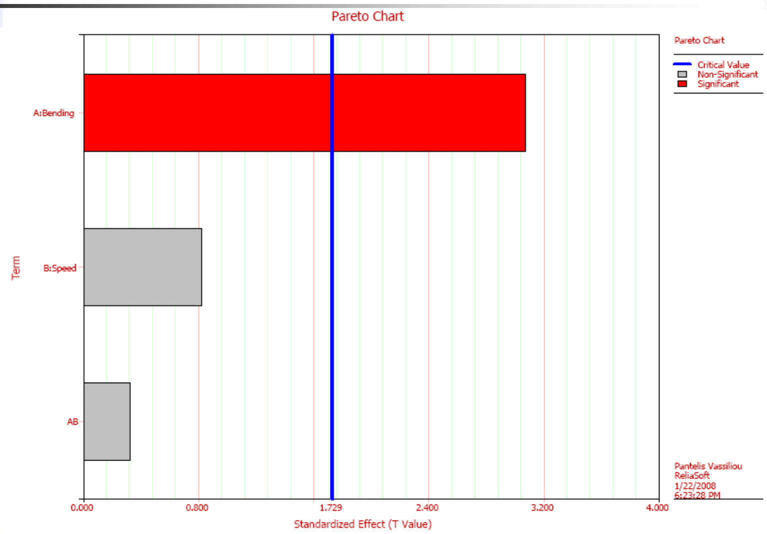
- Robust Design is an approach that reduces the sensitivity of product design to anticipated variation from environment or manufacturing without eliminating the causes



- One of the tools for the Robust Design is the Design Of Experiments (DOE)



Robust Design - DOE



Health Monitoring

- *Health Monitoring* refers to built in analysis dedicated for prediction of a failure before it affects the user
- A gradual trend or sudden raise or drop in a monitored value can point on a future need to tune, calibrate or replace a component before it leads to a more significant failure
- The benefit of *Health Monitoring* is to predict end of life of units exhibiting wear out mechanism
- Data for system *Health Monitoring* can be taken out of dedicated sensors or even periodic calibration results

Gertron גרטרון בע"מ

Simulations

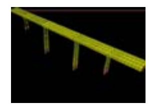
- Simulation in general, as well as the so called "Monte Carlo Simulation" or "Discrete Event Simulation" is a surprisingly simple concept to grasp.
- It involves the use of repeated experiments (simulation) to answer complex problems.
  - It has been referred to as "a poor man's mathematician."
- It can be computationally expensive to use.
  - However with increased computer power this is becoming less and less of an issue.

Gertron גרטרון בע"מ

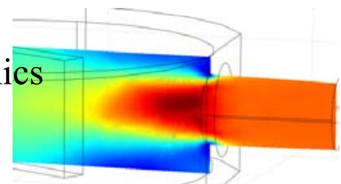
Simulations - Examples

- Finite Element Analysis (FEA)

- Dynamic Simulation



- Computational fluid dynamics (CFD)



Summary - Design

- RBD
- FTA
- MARKOV
- Reliability Allocation
- Reliability Prediction
- FMEA
- Stress-Strength Analysis
- Derating
- Robust Design
- Health Monitoring
- Simulations

Questions?

Agenda

- *Metrics*
  - Reliability
  - Failure Rate
  - MTTF / MTBF
  - Expected Life
  - MTTR
  - Availability
  - Reliability Growth
- *Toolbox*
  - Design
  - Tests
  - Monitor
- *Reliability Assurance Plan*
- *summary*

Tests

- The primary objective of reliability life testing is to obtain information concerning failures in order to quantify reliability, to determine whether reliability goals are being met, and to improve product reliability

ALT - Accelerate Life Testing

- The amount of time available for testing is often considerably less than the expected lifetime of the component
- This is certainly true for highly reliable components, for which testing under normal conditions would generate few if any failures within a reasonable time period

ALT

- In order to identify design weaknesses within reasonable amount of time, one or more of the following may be necessary:

Action	*MTBF*	*LE**
Increase the number of units on test	✓	✗
Accelerate the number of cycles per unit of time	✓	✓
Increase the stresses that generate failures (accelerated stress testing)	✓	✓

* Life Expectancy

ALT

- The three options above can be combined.
- Option #1 can not be use to accelerate **expected life** verification.
- All three option can be use to increase level of confidence

ALT - Examples

- Motors that are expected to operate for only a few hours a day in the field can be operated continuously with intermittent starting and stopping during testing
- Some wear out failure modes, such as corrosion, can be accelerated by operating the system under elevated stress levels such as higher temperature and humidity

- caution!
  - Increased mechanical stress, higher voltage or current, and increased radiation may accelerate other failure modes

ALT – Acceleration Rational

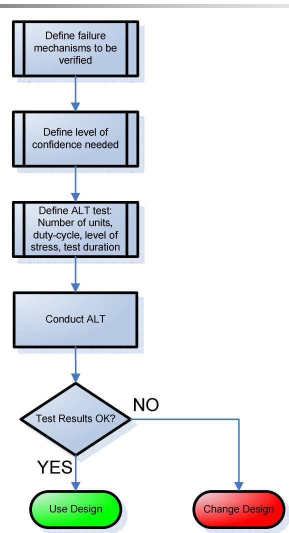
- The basic assumption of accelerated stress testing is:
  - That at the higher stress levels the same failure mechanism will be present and act in the same manner as at normal stress levels
  - No new failure modes are introduced
  - Failures will happen more quickly

ALT – When?

- Conduct an ALT to find dominant failure mechanisms and/or…
- …when there is a wear-out mechanism involved

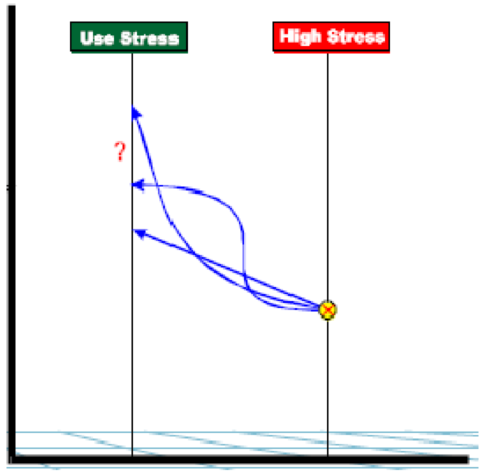
Confidential 51

ALT - Workflow



Confidential 52

Acceleration Models

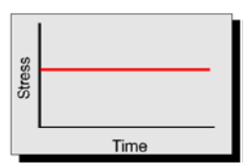


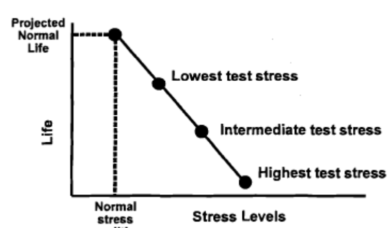
Confidential 53

Acceleration Models (cont.)

- The simplest case assumes a linear (constant) acceleration effect over time.
  That is, letting
  - t_n = time to failure under normal stress
  - t_s = time to failure at high stress level
  - then

$$AF = \frac{t_n}{t_s}$$





- where AF is an acceleration factor to be determined
- This is true (≈) only for Duty-Cycle Acceleration!!!

Confidential 54

Acceleration Models (cont.)

- *Arrhenius Model*
  The Arrhenius life relationship is widely used to model product life as a function of temperature
- Use to describe many products that fail as a result of degradation due to chemical reactions or metal diffusion
- Application
  - Electrical insulation and dielectrics
  - Solid state and semiconductor devices
  - Battery cells
  - Plastics
  - Incandescent lamp filaments

Acceleration Models (cont.)

- *Arrhenius Model*
  - When failures are accelerated primarily as a result of an increase in temperature, a common approach is based on the Arrhenius model:

$$A_F = e^{\frac{E_a}{k}\left[\frac{1}{T_O} - \frac{1}{T_S}\right]}$$

$$AF \approx 2^{\Delta T/10}$$

- A_F - Acceleration Factor
- E_a - Activation Energy (0.4 to 1.5)
- K - Boltzmann's Constant
- T_O - Operating Temperature [Kelvin]
- T_S - Accelerated Temperature [Kelvin]

Acceleration Models (cont.)

- *Inverse Power Relationship*
  The inverse power relationship is widely used to model products life as a function of an accelerating stress
- Application
  - Electrical insulation and dielectrics
  - Ball and roller bearings
  - Incandescent lamps
  - Flash lamps
  - Simple metal fatigue due to mechanical loading

Acceleration Models (cont.)

- *Coffin-Manson relationship*
  This inverse power law is used to model fatigue failures of metals subjected to thermal cycling
- *Palmgren's equation*
  This inverse power law is used to model roller and ball bearings life employing high mechanical load

Acceleration Models (cont.)

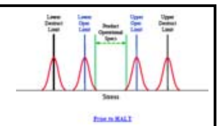
"All models are wrong, but some are useful."

George Box

Gertron גרטרון בע"מ

Confidential 59

HALT



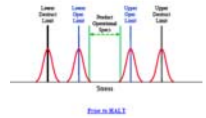
Highly Accelerated Life Testing

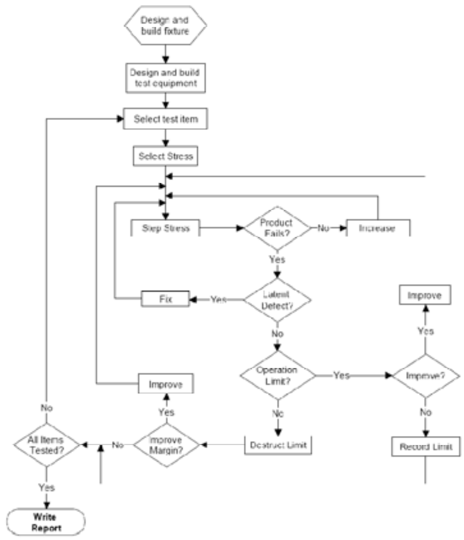
- HALT is a method of increasing the reliability of a product by gradually increasing stresses until the product fails.
- HALT is good for finding design weakness.
- HALT does not work well when there is a wear-out mechanism involved (use ALT for wear out mechanism).

Gertron גרטרון בע"מ

Confidential 60

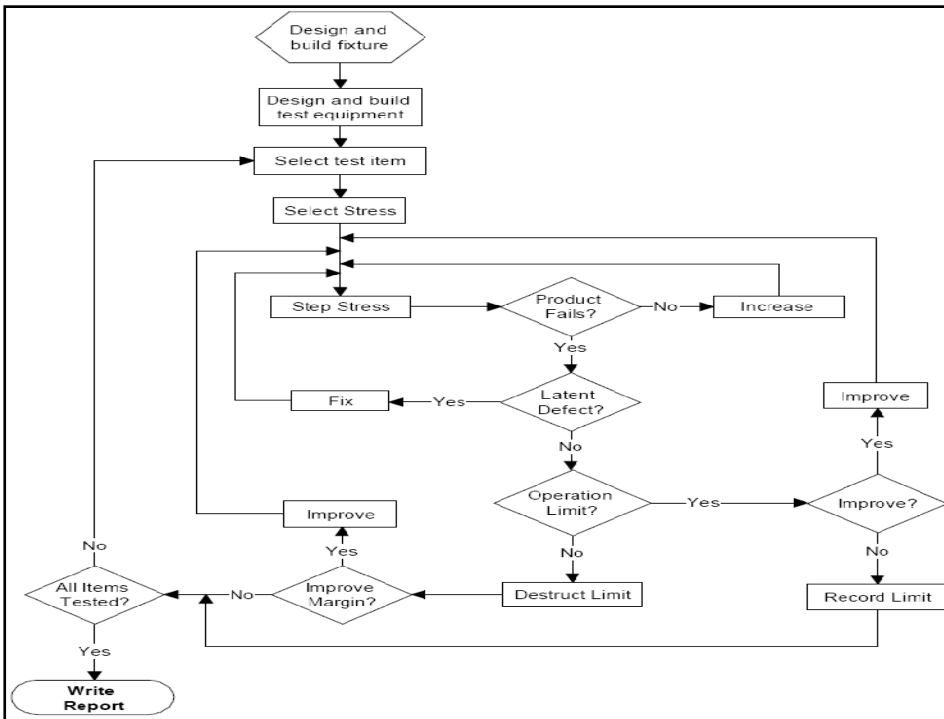
HALT - Workflow



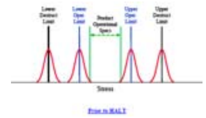


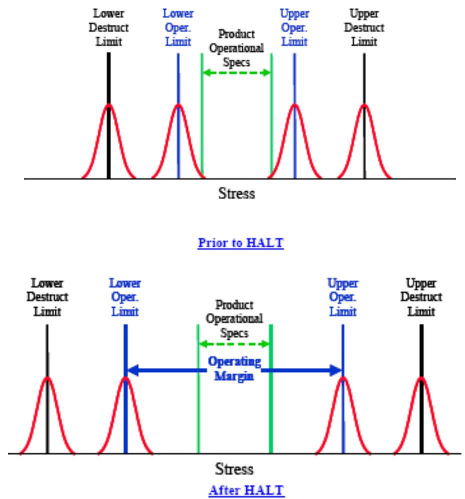
Confidential

61



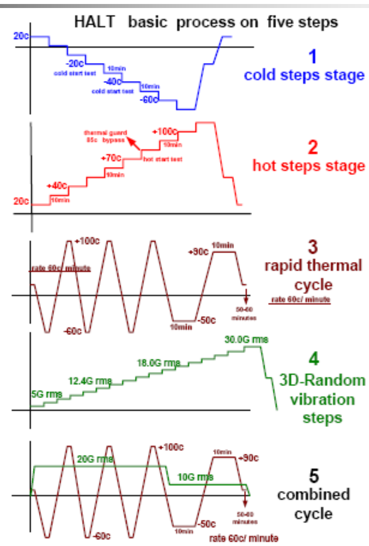
HALT - Benefit





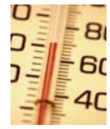
Confidential

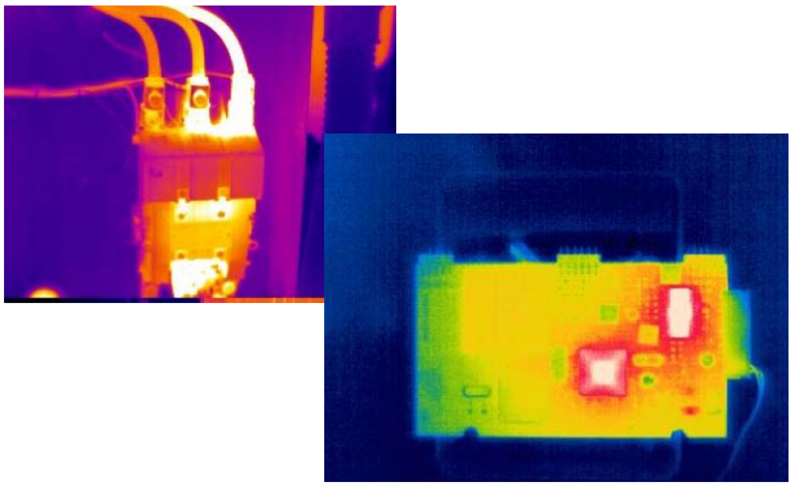
HALT - Process



Confidential

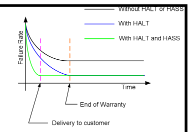
Thermal Imaging





Burn-In

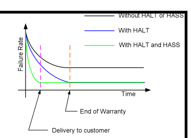
- Burn-in is a technique used to increase the Reliability of components and systems by operating the item under normal or accelerated environmental conditions prior to shipment
- If a burn-in procedure is effective, the weak population in the product should be eliminated
- The commonly used criteria for evaluating the effectiveness of burn-in testing are:
  - maximum mean residual life
  - Maximum probability of mission success after burn-in
  - Cost is also often considered as one of the objectives



HASS

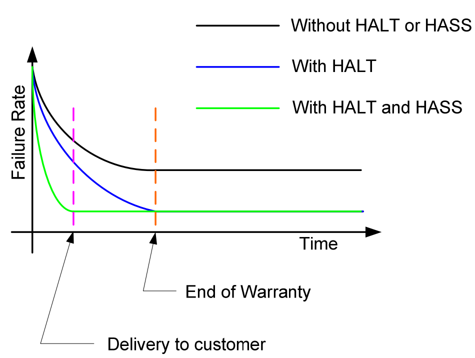
Highly Accelerated Stress Screening

- HASS is the most effective reliability screening method: it requires very little time, with typical three hours screening cycle, far less than the typical 48-hour required for regular burn-in
- The HASS process screens out not only infant mortality failures, but it also accelerates potential device defects and identifies manufacturing process flaws

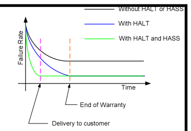


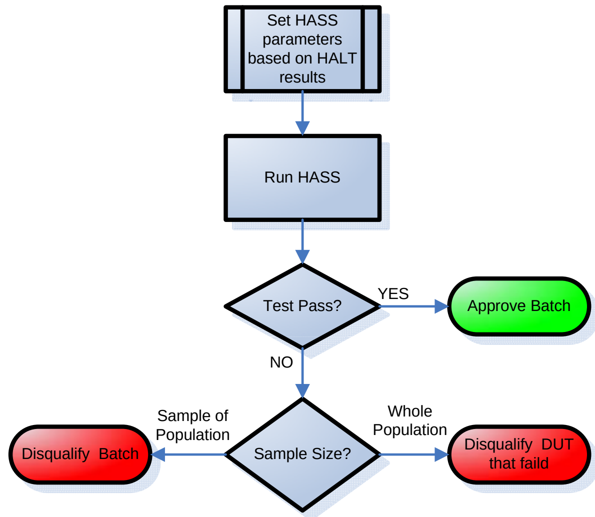
HASS

- HASS relies on HALT results
- HALT helps identifying the combinations of stresses that most effectively force weaknesses to manifest as detectable failures

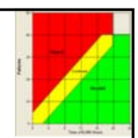


HASS - Workflow

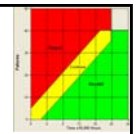




RDT

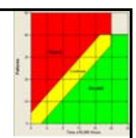


- ***Reliability Demonstration Tests*** are long duration physical stress tests which measure full product reliability and accelerate failure mechanism
- During RDT execution, recorded results are reviewed on a regular basis to guide decision on declaring it successful, continuing, modifying, or abandoning the test



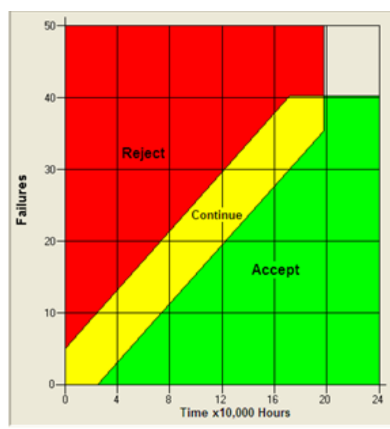
SPRT

- One of the more common test methods is the ***Probability Ratio Sequential Test*** (PRST), also known as ***Sequential Probability Ratio Test*** (SPRT)
- The SPRT is a method of testing for reliability that minimizes the number of test units and test time needed to demonstrate a required reliability



SPRT

- The **Green** area in the graph represents a low failure rate: If the accumulated number of failures per the elapsed time reaches below a certain predefined ratio (represented by the **green** area), the test can be stopped with positive results
- The **Red** area represents a high failure rate, and accordingly upon reaching that area the test is stopped with negative results
- The **Yellow** area represent a continuous failure rate that cannot represent either high or low reliability, thus the **test should be continued**



Summary - Tests

- ALT
- HALT
- Thermal Imaging
- Burn-In
  - HASS
- RDT
  - SPRT

Confidential 73

Questions?

Confidential 74

Agenda

- *Metrics*
  - Reliability
  - Failure Rate
  - MTTF / MTBF
  - Expected Life
  - MTTR
  - Availability
  - Reliability Growth
- *Toolbox*
  - Design
  - Tests
  - Monitor
- *Reliability Assurance Plan*
- *Summary*

"You cannot manage what you cannot control, and you cannot control what you cannot measure"

Source unknown

FRACAS

- ***Failure Reporting, Analysis and Corrective Action System***
- FRACAS is the main source for systems reliability metrics
- FRACAS is used to track and analyze failures associated with products during their useful life. Such follow up is essential for reliability sustaining and growth

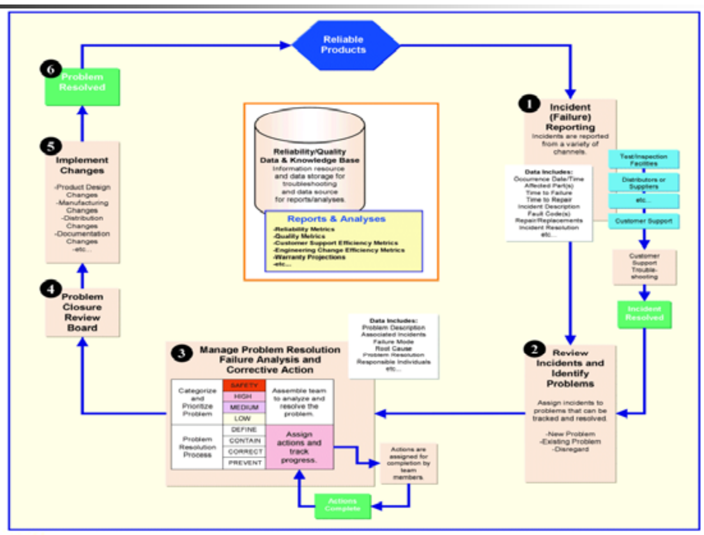
FRACAS

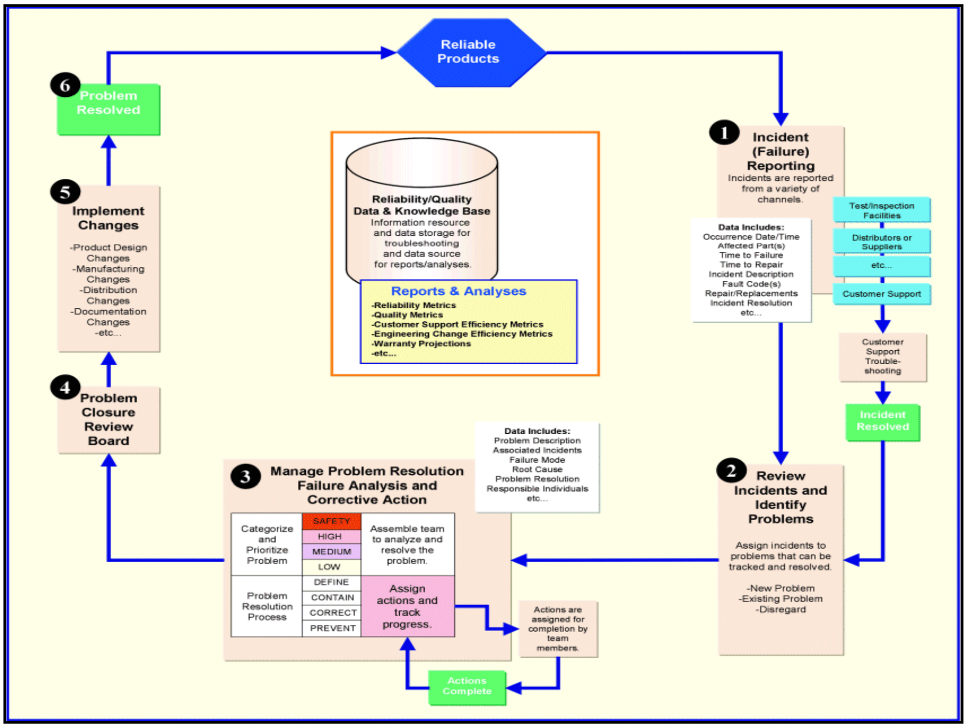
- The essence of FRACAS is closing the loop back to the developer:
  - Failures and faults (of both hardware and software) are properly reported and analyzed, enabling to understand the failure cause.
  - Positive corrective actions are identified, implemented and verified to prevent further recurrence of such failure

FRACAS

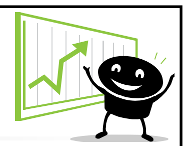
- For effective analysis, it is very important to well define the resolution codes, avoiding a situation where either more than one resolution code can be used or none.
- The list of possible resolution codes must have neither too many nor too few codes

FRACAS





Reliability Growth – Why?



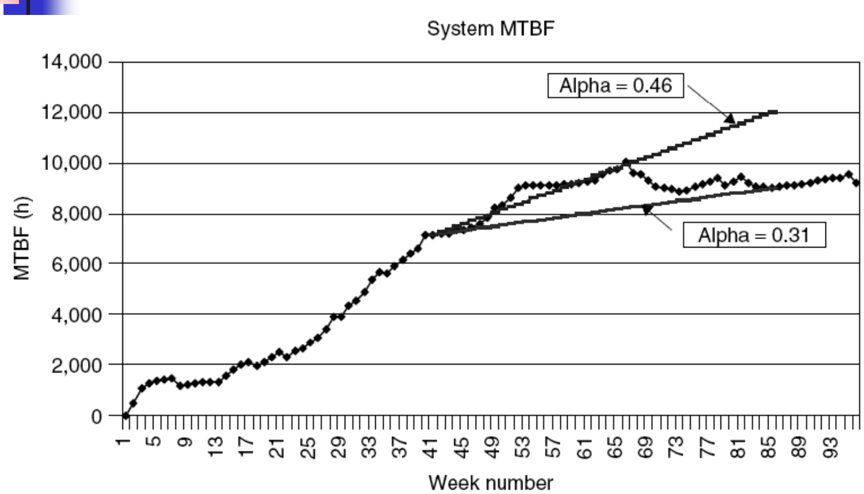
- Reliability goals become more and more demanding…
- Validating higher reliability requires much longer test time…
- Development cycles becomes more and more shorter…
- …AS a result, systems are launched with low reliability and an aggressive Reliability Growth Plan need to be enforced
- Metrics:
  - Duane Plot (Alpha)

Gertron גרטרון בע"מ

Reliability Growth - Definition

- Reliability growth is the improvement in the reliability of a product (component, subsystem or system) over a period of time due to changes in the product's design and/or the manufacturing process

Duane Plot



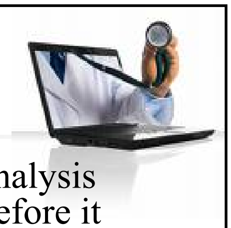
Duane Plot - Alpha

- 0.4 ÷ 0.6 A top priority program is in effect to eliminate failure modes. Immediate attention and corrective actions prevail.
- 0.3 ÷ 0.4 An above average program on reliability improvement exists. There is a well managed plan and action on important failure modes.
- 0.2 ÷ 0.3 Routine attention is paid to reliability improvement. No environmental testing. Action taken on important failure modes only.
- 0.0 ÷ 0.2 A low priority in reliability improvement.

Gertron גרטרון בע"מ

Confidential 85

Health Monitoring



- *Health Monitoring* refers to built in analysis dedicated for prediction of a failure before it affects the user
- A gradual trend or sudden raise or drop in a monitored value can point on a future need to tune, calibrate or replace a component before it leads to a more significant failure
- The benefit of *Health Monitoring* is to predict end of life of units exhibiting wear out mechanism
- Data for system *Health Monitoring* can be taken out of dedicated sensors or even periodic calibration results

Gertron גרטרון בע"מ

Confidential 86

Summary - Monitor

- FRACAS
- Reliability Growth
- Health Monitoring

Questions?

Thanks for your attention