Reliability Program Overview for Developers
Failures

Amnon Ganot - September, 2010

Agenda

- *Overview*
- *Quality & Reliability*
  - Quality Definition
  - Reliability Definition
  - Unreliability Cost
- *Failure*
  - Definition
  - Sources
  - Types
  - Failure Mode
  - Failure Mechanism

"To design systems that work correctly we often need to understand and correct how they can go wrong"

Dan Goldin, NASA Administrator, 2000

Failure Definition

- Concise Oxford English Dictionary:
  - *Lack of success*
    *Action of **ceasing to function** or state of **not functioning**.*
- Wikipedia English:
  - *In general, failure refers to state or condition of **not meeting desirable or intended objective**, may be viewed as **opposite of success**.*
- Telecommunication Standard Terms:
  - ***Temporary or permanent termination** of ability of an entity to perform its **required function**.*

Why do products fail?

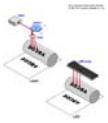
- When a failure occurs, and the failure mode is analyzed to determine its root cause, it is nearly always the result of human error.
- Therefore, failures are caused by errors made by people such as systems engineers, design engineers, production personnel, users and maintenance personnel.
- Product failures are caused by people, not by parts!
- Why do people make mistakes?
  - Human nature
  - Complexity of engineering
- Further analysis will suggest that all failures, in theory and almost always in practice, can be prevented.

Failure(?) Examples

- No light from tungsten lamp after 100 hours
- No light from tungsten lamp after 800 hours
- No light from tungsten lamp after 1100 hours
- Tire is flat

- Motor is noisy
- Car stopped due to lack of fuel

- Paper jam in printer
- Fan rotation speed decreased by more than 20% comparing with its original rotation speed at start
- LED/LASER intensity decreases by more than 20% comparing with its original intensity at start



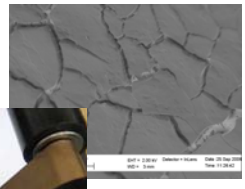
Agenda

- *Overview*
- *Quality & Reliability*
  - Quality Definition
  - Reliability Definition
  - Unreliability Cost
- *Failure*
  - Definition
  - Sources
  - Types
  - Failure Mode
  - Failure Mechanism

Source of Failures - Internal

- Design Failures
  - Over Load - Mechanical

- Mechanical components wear out due to friction, overload, plastic deformation, fatigue, changes in composition due to excessive heat, corrosion, abuse, *etc*.



Source of Failures – Internal (cont.)

- Over Load – Electrical
  - Overload currents are typically 5 to 20 times normal current and include starting currents for large motors, inrush currents for incandescent lamps, and so forth.
  - Ripple current is the RMS value of alternating current flowing through a capacitor. This current causes an internal temperature rise due to power losses within the capacitor
- Unused IC legs
  - Behaves like small antennas and convert electric and magnetic field to voltage and current that change IC behavior or impair it

Gertron גרטרון בע"מ

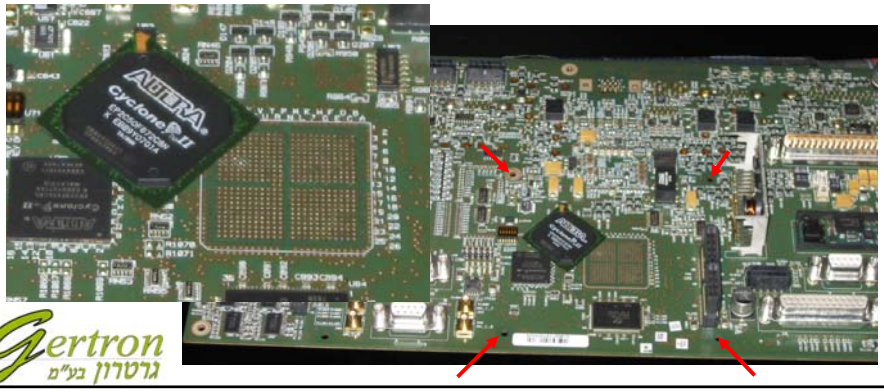
Source of Failures – Internal (cont.)

- PCB Design
  - Since components in electronics equipment experience a range of temperatures during service, then the *coefficient of thermal expansion* (CTE) is important, particularly where materials are fixed together, as in the case of solder joints.
  - The generation of stress and strain under conditions of changing temperature, when materials with different thermal expansion coefficients are joined, is the principal cause of failure of soldered joints in service.
  - The impact of ROHS on PCB reliability: Higher soldering temperatures ~220°C Vs ~180°C) yield higher thermo-mechanical stress.

Gertron גרטרון בע"מ

Source of Failures – Internal (cont.)

- PCB Design (cont.)
  - PCB securing locations Vs connector's locations might induce mechanical stresses while connecting and disconnecting the connectors on the board.



Gertron גרטרון בע"מ

Source of Failures – Internal (cont.)

- Robotic Cables

- Cabling is one element of robotic work cells that is often overlooked during the design phase. Cables are often just an afterthought in work cells
- Without proper planning, cable wear can be one of the first things to cause downtime on a robot work cell.
- Frequently, standard cabling is used where high-flex cable is required

Gertron גרטרון בע"מ

Source of Failures – Internal (cont.)

- Robotic Cables (cont.)
  - Often, cables are tied down too tightly with tie wraps on something that is moving
  - Another common problem is overfilling cable carriers and cable tracks
  - Inaccurately underestimating the bend radius that the cable needs to be put through causes cracks and conductors to fail

Source of Failures – Internal (cont.)

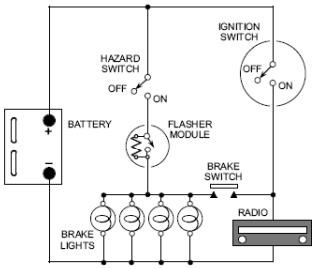
- Snake Circuit
  - *A sneak condition is a latent hardware, software, or integrated condition that may cause an unwanted event to occur or may inhibit a desired event and is not caused by component failure*
  - *These conditions are characterized by their random nature and ability to escape detection during the most rigorous of standardized system tests*
  - *Sneak conditions can cause improper operation, loss of system availability, program delays, or even death or injury to personnel*

Source of Failures – Internal (cont.)

- Snake Circuit - Example

1. Auto Brakes, Flasher and Radio
(Some autos — late '60s Refs. 3, 4, & 5)…

- **REQUIREMENTS:** Radio cannot be left ON with ignition switch OFF. Hazard flasher must be operable with ignition switch OFF.
- **DESIGN:** Radio is in series with ignition switch. Hazard switch and flasher bypass ignition switch.
- **SCENARIO:** Radio operates synchronously with brake lights when ignition switch is used to turn off radio, hazard flasher is operated, and brake pedal is depressed.



FIND THE SNEAK!

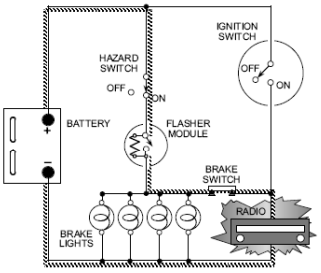
Source of Failures – Internal (cont.)

- Snake Circuit – Example (cont.)

1. Auto Brakes, Flasher and Radio
Sneak Disclosed…

SNEAK: Brake switch provides reverse-current path, placing radio in parallel with brake lights.

- **Is this a *true* Sneak Circuit?**
  - **Will it cause *harm?***
    - **How might it be *corrected?***



Source of Failures – Internal (cont.)

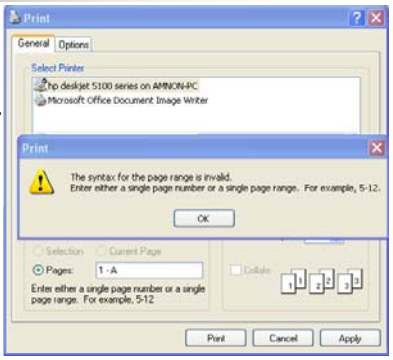
- Bouncing (Relays)
  - Contact bounce (also called *chatter*) is a common problem with mechanical switches and relays
  - When the contacts strike together, their momentum and elasticity act together to cause bounce.
  - The result is a rapidly pulsed electrical current instead of a clean transition from zero to full current
  - Some analogue and logic circuits that respond fast enough to misinterpret the on-off pulses as a data stream
  - Bouncing contacts often cause the contact surfaces to weld.

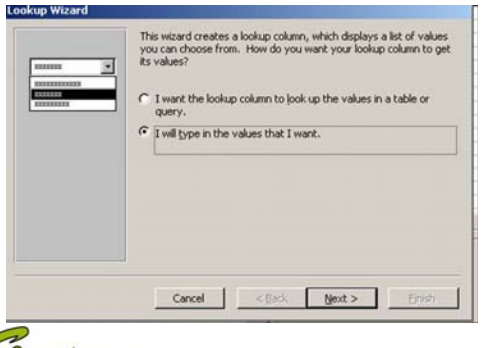
Source of Failures – Internal (cont.)

< back

Source of Failures – Internal (cont.)

- Graphic User Interface
  - Input parameters sanity check.
  - Input command buffer





Source of Failures – Internal (cont.)

- COTS* / Purchase Shelf Items
  - All possible design causes as well as manufacturing, transporting, storage, usage and maintenance
  - Equal efforts should be expended on both the subsystems that you make as well as the ones you acquire from suppliers.
  - Don't just award the lowest bidder

** COTS – Commercial Off The Shelf*

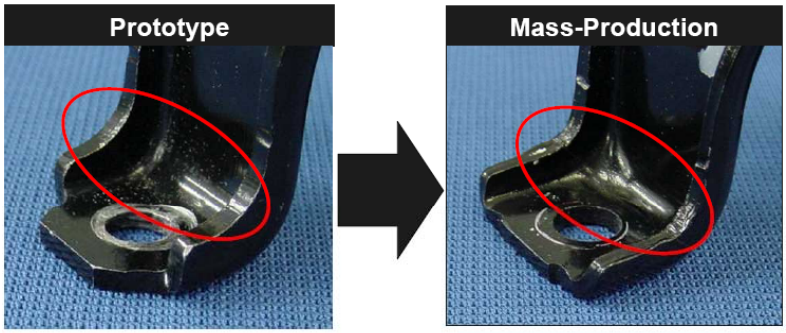
Source of Failures - External

- Manufacturing
  - The inherent reliability of the design will degrade when deployed through manufacturing into field service
  - Once you have a reliable design, you must make sure the manufacturing process is also "reliable"!

Source of Failures – External (cont.)

- Example: Production Change

Stabilizer Bracket Made by an Automotive Company



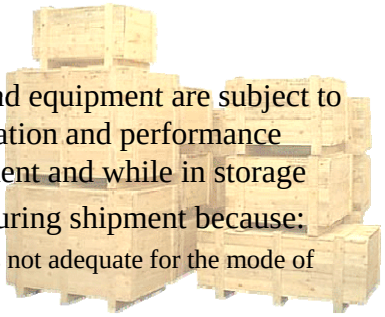
Fatigue life reduced by a factor of 10!

Source of Failures – External (cont.)

- Example: Particles in Hard Drives
  - Problem caused in manufacturing:
    - Scratches on hard drive because of particles caused by driving screws during assembly
  - Corrective actions:
    - Design control
      - Improve screw material
    - Supplier control
      - Monitor screw material
    - Manufacturing control
      - Improve cleanliness of screw holes
      - Monitor particles

Source of Failures – External (cont.)

- Transporting & Storage
  - Electronic components and equipment are subject to change, damage, deterioration and performance degradation during shipment and while in storage
  - Defects can be induced during shipment because:
    - the packing protection was not adequate for the mode of transportation
    - the container or other packaging material did not meet specification requirements
    - the equipment was roughly handled or improperly loaded



Source of Failures – External (cont.)

- Shock and vibration, which are present in all modes of transportation, can cause wire chafing, fastener loosening, shorting of electrical parts, component fatigue, misalignment, and cracking
- Lubricants, used on the bearing surfaces of relays, solenoids, and motors deteriorate over time
- Over a period of time, many plastics (such as those used in the fabrication of electronic components, i.e., integrated circuits, capacitors, resistors, transistors, etc.) lose plasticizers or other constituents which may evaporate from the plastic, causing it to become brittle, and possibly, to shrink

Source of Failures – External (cont.)

- Electronic components age and deteriorate over long storage periods due to numerous failure mechanisms:

Capacitors	Moisture permeates solid dielectrics and increase losses which may lead to breakdown
Resistors	The value of composite-type fixed resistors drift, and these resistors are not suitable at temperatures above 85 °C
Semiconductors	Plastic encapsulated devices offer poor hermetic seal, resulting in shorts or opens caused by chemical corrosion or moisture
Connectors	Corrosion cause poor electrical contact and seizure of mating members. Moisture cause shorting at the end
Transformers	Windings corrode causing short or open circuiting

Source of Failures – External (cont.)

- Usage
  - Site Preparation – Environmental
    - Temperature - extremes & gradients
    - Humidity extremes
    - Humidity and Temperature combination – Due point
    - Vibration (floor) – spectrum (amplitude & frequency, all axes)
    - Line Voltage – extremes, spikes etc.
    - Air Supply – pressure extremes, fluctuation, cleanness, etc.
    - Electro Static (Human!)
      - In an ESD event, the human body can reportedly generate static charge levels as high as 15,000 volts by simply walking across a carpeted floor and 5,000 volts by walking across a linoleum floor
    - Electro Magnetic Interference

Source of Failures – External (cont.)

- Training
  - Reliability at the customer point of view is a subjective measure
  - Non-consistence behavior of a system is perceived as unreliability even if it is due to wrong operation of the system
  - For example, if an instruction of warming the system for a certain time (to achieve full accuracy) is not followed, than, from time to time, full performance is not reached

Source of Failures – External (cont.)

- Human Factors (Foolproof)
  - Human factors are important components which directly influence the product's quality and reliability, especially safety
  - Any operation that relies on the human element will run into the problem of errors
  - Human beings are famous for not following instructions (or even reading them)
  - Workmanship during manufacture is another human consideration for the designer
  - Designs which require a high degree of workmanship may be very difficult to produce and thus, the reliability is impacted
  - Workmanship concerns generally affect the "infant mortality" portion of the reliability curve

Source of Failures – External (cont.)

Source of Failures – External (cont.)

- Maintenance
  - Maintainability is another human factor concern in that the device should be maintainable easily by the operators & service personal
  - There are many examples of poor reliability that can be traced to poor maintenance

Source of Failures – External (cont.)

www.haaretz.co.il

עודכן ב- 28/06/2009 10:06

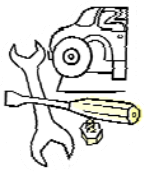
הכמעט-התרסקות בנתב"ג לפני שלושה שבועות:
הטייסים פעלו בניגוד לנוהל

כשל חמור ביישום נוהל נחיתת מכשירים בנמל התעופה בן גוריון, נחשף בחקירת אירוע בטיחות הטיסה שבו כמעט התרסקו לפני כשלושה שבועות שני מטוסי נוסעים, של אל-על וישראייר. בזמן ששני המטוסים התקרבו לנחיתה, נודע להם על תקלה במכשיר ה-ILS המסייע בנחיתה, אך הם פעלו בניגוד לנוהל הישראלי במקרה זה - כך עולה בדו"ח חקירת ביניים שהוצגו בישיבה אצל מנהל רשות התעופה האזרחית גיורא רום. ביום חמישי נמנעה תאונה נוספת, כשמטוס טורקי המריא לעבר מטוס שהתקרב לנחיתה.

רשות שדות התעופה (רש"ת) החלה בחקירת האירוע. אחת האפשרויות שנבדקות היא אם צמחייה עבותה וגבוהה באזור מכשיר העזר לניווט בנתב"ג, שיבשה את הקרן והאותות לפיהן הנמיכו מטוסי הנוסעים לנחיתה. לאחר שהתגלתה התקלה, נכשל ניסיון ראשון לאפס את המכשיר ורק לאחר שנוקה השטח חזר המכשיר לפעול כסדרו.

Source of Failures – External (cont.)

- Reduction of Maintenance
  - Reduce the need for maintenance, as much as possible. Self-oiling, sealed bearings, built in self-checks, etc. are methods of reducing maintenance requirements on operators and service engineers.
- Ease of Maintenance
  - Maintenance tasks should be made as convenient as possible for the operator and the service engineer. Considerations should include disassembly using one tool, all maintenance items on a uniform schedule, high level of testability



Questions?

Agenda

- *Overview*
- *Quality & Reliability*
  - Quality Definition
  - Reliability Definition
  - Unreliability Cost
- *Failure*
  - Definition
  - Sources
  - Types
  - Failure Mode
  - Failure Mechanism

Failure Types – Time Wise

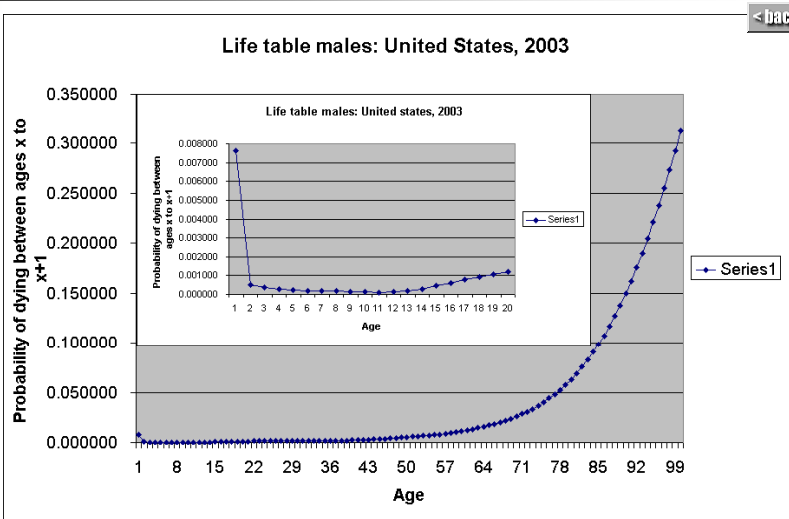
- Failures can be broken into basically three distinct and separate classes of failures; early-life, event-related, and wear out
- Early-life failures, also known as *infant mortalities*, are the result of defects introduced during the manufacturing or assembly process
- The useful life period is characterized by a relatively constant failure rate caused by randomly occurring events
- Wear out failure mechanisms occur as a result of prolonged exposure to operational or environmental stresses and will occur in the entire population of items if they are in service long enough

Failure Types – Time Wise (cont.)

- Infant Mortality
  - The infant-mortality period represents a small portion of the shipped population which fails usually in the first year and do not immediately show up during screening
  - Failures occurring in the initial phase of deployment usually result from built-in flaws due to faulty workmanship, transportation damage or installation errors

Failure Types – Time Wise (cont.)

< back



Failure Types – Time Wise (cont.)

- Causes of infant-mortality failures include:
  - Inadequate quality control
  - Uncontrolled manufacturing processes
  - Inadequate component and system test specifications
  - Component and system design deficiencies
  - Material deficiencies
  - Improper handling and packaging
  - Incorrect setup, installation, or procedures
  - Incomplete testing

Failure Types – Time Wise (cont.)

- Infant-mortality failures can be reduced by monitoring and controlling the manufacturing process (Burn-in / ESS / HASS)
- Failure analysis is vital during this phase to identify and correct the causes of problems so they can be eliminated prior to deployment

Failure Types – Time Wise (cont.)

- Useful Life
  - The useful life period is normally characterized by relatively infrequent and unpredictable failures
  - Failures occurring during the useful life period are referred to as *random failures* because of this infrequent and unpredictable nature
  - That is not to say, however, that the failures do not have a specific root cause, or that the occurrence is unavoidable

Failure Types – Time Wise (cont.)

- Causes of useful life failures include:
  - Inadequate component or system design margins
  - Misapplication
  - Latent component and system defects
  - Excessive electrical, thermal or physical stress (beyond design limits)

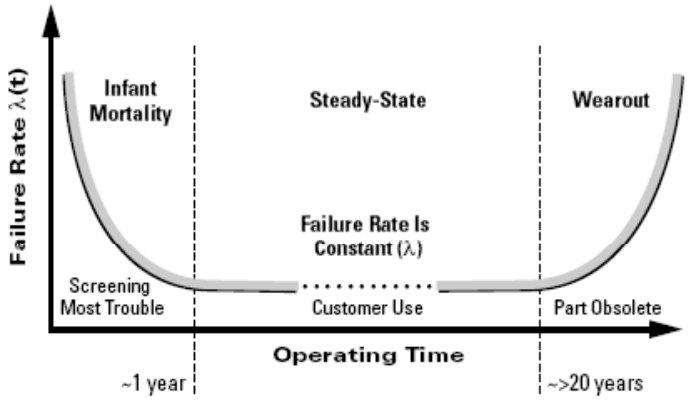
Failure Types – Time Wise (cont.)

- Wear Out

  - The failure rate of a component will increase rapidly in the wear out phase
  - Wear out failures are due primarily to the deterioration of the design strength of a device resulting from the operation and exposure to environmental fluctuations
  - This deterioration may result from various physical and chemical phenomena that include:
    - Corrosion/oxidation
    - Insulation breakdown
    - Frictional wear or fatigue
    - Shrinking/cracking of plastic materials
    - Metal migration
  - Wear out failures may be reduced or eliminated through preventive maintenance and by providing adequate design margins to extend the life of components

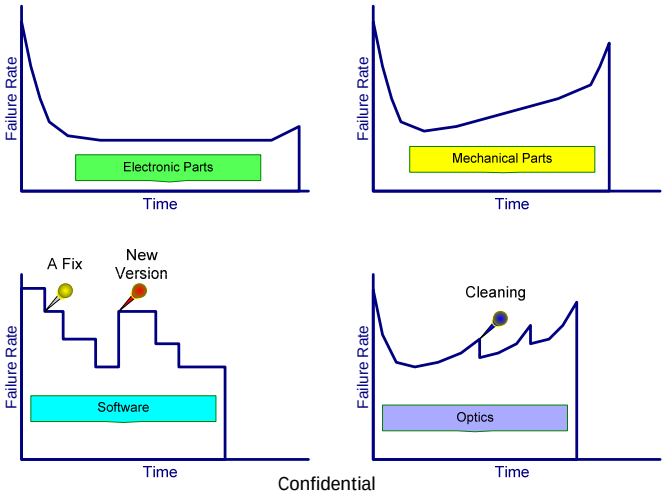
Failure Types – Time Wise (cont.)

- Bathtub



Failure Types – Time Wise (cont.)

- Bathtub Types

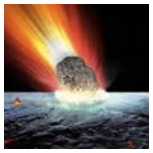


Failure Types – Severity Wise

- The *potential effect* of a failure is defined as the impact of the failure on the function of neighboring components and higher-level systems
- The end effect of a failure is assessed in terms of severity

Failure Types – Severity Wise (cont.)

- Catastrophic (Mission)
  - A failure that may cause *sever injure* or major *system damage*
    - Example: Loss of car brakes



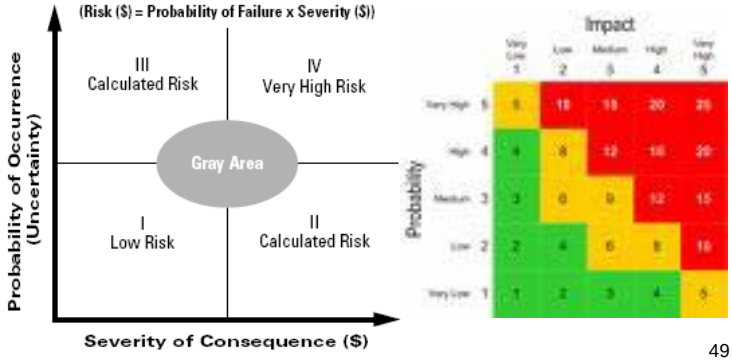
- Critical (Mission)
  - A failure that may cause *minor injury* or inability to perform *primary mission*
    - Example: An office illumination failure

Failure Types – Severity Wise (cont.)

- Major / Significant (Limping)
  - A failure that may cause *degradation* in mission performance (parametric failure)
    - Example: Office air conditioning system is down
- Minor (redundancy)
  - A failure that does not influence system performance but may result in *unscheduled maintenance*
    - Example: Car hand-brake is broken

Failure Types – Severity Wise (cont.)

- Risk Value
  - This value is defined mathematically as the probability of failure times severity costs



Questions?

Agenda

- *Overview*
- *Quality & Reliability*
  - Quality Definition
  - Reliability Definition
  - Unreliability Cost
- *Failure*
  - Definition
  - Sources
  - Types
  - Failure Mode
  - Failure Mechanism

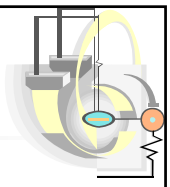
Failure Mode - Definition

- The manner in which a unit / system fails.
- A failure mode is defined as the consequence of the mechanism through which the failure occurs, i.e., the manner by which the failure is observed.

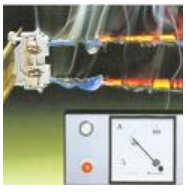
Failure Mode

- When designing systems containing electronic components, it is valuable to an engineer to have the knowledge of component failure modes and mechanisms and their probability of occurrence. These factors are also invaluable to an analyst when performing failure analyses and developing recommendations to eliminate the future occurrence of failures

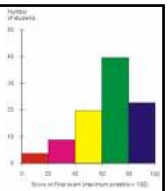
Failure Mode – Examples



- Technological - Electronic or electrical components may fail in any of the following modes:
  - *Short circuit:* Diodes, transistors, capacitors may often fail in this mode.
  - *Open circuit*: Resistors, crystals, *etc*. may often fail in this mode.
  - *Degraded performance:* SCRs and capacitor aluminum may fail in this mode.
  - *Functional failure:* Coils and relays may often fail in this mode.



Failure Mode – Distribution

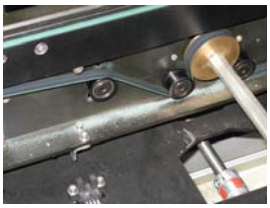


- A unit, assembly or system can fail often in more than one failure mode.
- In fact the relative frequency of occurrences of these failure modes can be different for different component types and these failure modes and their relative frequencies should be considered for a particular type of application of a component during the design of a system using these components

Failure Mode – Distribution (cont.)

Device Type	*Failure Mode*	*Failure Mode Probability*
Capacitor, Ceramic	Short	0.49
	Change in value	0.29
	Open	0.22
Diode, general	Short	0.49
	Open	0.36
	Parameter change	0.15
Power Supply	No output	0.52
	Incorrect output	0.48
Sensor	Erratic output	0.58
	Short	0.20
	Open	0.12
	No output	0.10

Failure Mode – Distribution



Device Type	*Failure Mode*	*Failure Mode Probability*
Belt	Excessive Wear	0.75
	Broken	0.25
Cable	Short	0.45
	Excessive Wear	0.36
	Open	0.19
Clutch	Binding/Sticking	0.56
	Slippage	0.24
	No movement	0.20

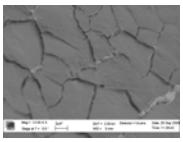
Questions?

Agenda

- *Overview*
- *Quality & Reliability*
  - Quality Definition
  - Reliability Definition
  - Unreliability Cost
- *Failure*
  - Definition
  - Sources
  - Types
  - Failure Mode
  - Failure Mechanism

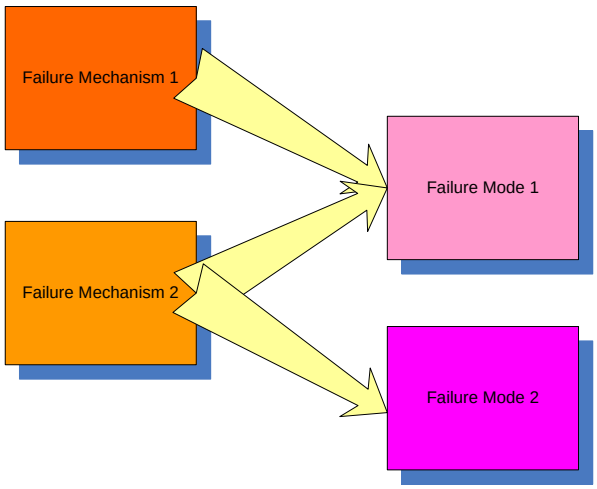
Failure Mechanism (Physics of Failure)

- Definition
  - A failure mechanism is a physical, chemical, thermal or metallurgical process that causes component characteristics to change beyond tolerance, which eventually leads to a certain mode of component failure.



  - Several failure mechanisms may exist simultaneously at a point of time, eventually leading to a failure of a component in a particular mode. Two or more same failure mechanisms can lead different failure modes. All failure modes are known as *primary failures*.

Mechanism to Mode correlation



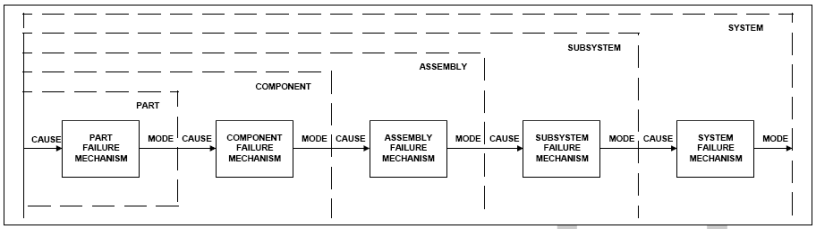
Failure Mechanism - Examples

- Fatigue is a major failure mechanism of mechanical parts including bearings and electrical contacts

Type	*Mechanism*	*Percent Failure Mode*
Microcircuit	Surface anomalies	35-70 Degradation
	Wire Bond	10-20 Open
	Seal defects	10-30 Degradation
Diode	Corrosion	20-40 Intermittent
	Lead/Die contact	15-35 Open
	Header bond	15-35 Drift
Capacitor	Connection	10-30 Open
	Corrosion	25-45 Drift
	Mechanical	20-40 Short

Cause & Effect

- A failure mechanism is the cause of a failure mode. A failure mode is the failure mechanism of the next level



Flaw, Fault & Failure

- Flaw - defect, imperfection
- Fault - an abnormal condition at the component, equipment, or sub-system level which may lead to a failure
- Failure - state or condition of not meeting desirable or intended objective
- *Example: A bad ventil in a car tire might cause loss of air pressure that might cause delay in arriving to destination*
- *More Examples:*
  - *Tadirans's Emergency Light Battery*
  - *Mazda 3*

Flaw, Fault & Failure

מאזדה 3 החדשה: מהומה על מאומה?

21.04.09 דני שטיינמן

המכונית המסקרנת ביותר עבורנו זוכה לכותרות שליליות בארץ כתוצאה מקריאה לתיקון בארה"ב. הכצעקתה?

אין ספק שמידע שכזה הנו משמעותי ורלוונטי עבורנו, אך עיון בנתונים ובעובדות מלמד אחרת. ראשית, הקריאה לתיקון יצאה ממאזדה-ארה"ב כבר ב-15 באפריל, ויועדה לרוכשי מאזדה 3 החדשה (מודל 2010) – בארה"ב. הקריאה מיועדת לכ-25,000 בעלי מאזדה שכבר נמכרו (ושלא כולם נמסרו בפועל ללקוחות) ובה מתבקשים בעלי הרכב לסור למוסכים בשל כשל פוטנציאלי שהתגלה. עיקרו של הכשל: מיקום בעייתי של חוט חשמל, שבתנאים מסוימים עלול להתחמם או אף להיות מותך ובכך לגרום לקצר שעלול לדומם את המנוע.

Gertron גרטרון בע"מ

Summary

- Failure Definition
- Why Products Fails?
- Failure Source
  - Internal
  - External
- Failure Types
  - Time Wise
  - Severity Wise
- Failure Mode
- Failure Mechanism
- Flaw, Fault & Failure

Gertron גרטרון בע"מ

Questions?

Thanks for your attention