Certified Reliability Engineer.

Ch 4. Reliability in Design & Development.

中国可靠性
KekaoXing.com

Industrial Engineering & Management Systems Research Center.

https://www.kekaoxing.com

Reliability Design Techniques.

Reliability Design Techniques

- Use Factors.
- Stress-Strength Analysis.
- FMEA/FMECA in Design.
- Fault Tree Analysis (FTA) in Design.
- Tolerance and Worst-Case Analysis.
- Robust-Design Approaches.
- Human Factors Reliability.
- Design for X (DFX)

Design Consideration.

[CRE Primer Ⅴ 2-3]

List of Design Considerations.

- Performance requirements.
- Environmental ranges.
- Specific measures (such as MTBF or failure per time interval)
- Diagnostics (built-in vs. external, self-diagnostic vs. expert.
- Repair (MTTR)
- Field service (repair centers, exchange parts, instruction manuals, etc.)
- Thermal analysis.
- Structural analysis.
- FMEA/Fault tree analysis.
- Maintainability analysis.
- Manufacturability analysis.
- Software/Circuit analysis.
- Electromagnetic compatibility (EMC)
- Computer modeling or Monte Carlo simulation.
- First design review.

Use Factors.

[CRE Primer Ⅴ 4-5]

Introduction.

- An organization must collect or generate customer information. This information may come from direct customer interviews, surveys, proposals, reports, concept proposals, project meetings, contract review, etc.

- The design requirements may be specified by customer, or may not be stated directly. This is, the customer states an intended use, but may not be fully aware of the consequences.

- Example.

Objective	Metric
Noise	No audible sound of slide opening
Slide mechanism	No visible corrosion
Slide mechanism	Stainless steel
Open and close	20 year life at rating of 50,000 repetitions.

Use Factors.

[CRE Primer V 4-5]

Some of the Use Factors.

- Air quality.
- Acceleration.
- Depth & velocity.
- Dew point.
- Air quality.
- Displacement.
- Duty cycle.
- Gas.
- Harmonics.
- Hydrological.
- Light.
- Lightning.
- Meteorological.
- Noise.
- Temperature range.
- Temperature cycling.
- Pressure.
- Humidity.
- Moisture.
- Wind.
- Dust.
- Sand.
- Solar radiation.
- Plant growth.
- Mold.
- Transportation vibration.
- Transportation shock.
- Electromagnetic radiation.
- Chemical (corrosive, pH)
- Biological.
- Time and motion.
- Voltage.
- Wind speed.
- Wind/solar.
- Electrostatic discharge.
- Radio-frequency interference.
- Overload.
- Storage.
- Power supply variation.
- Multiple factor interaction.

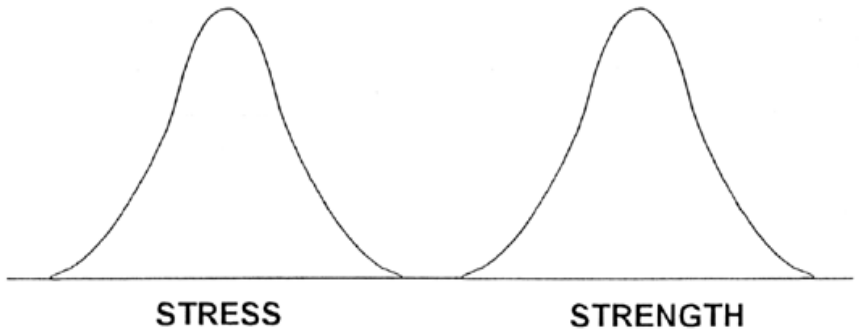
Stress-Strength Analysis.

Stress-Strength Interference.

- 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 nominals.

- **Stress-Strength Separation.**

  The distribution curves for stress and strength are far enough apart that there is little probability that a high stress level interfere with an item that is on the low end of the strength distribution.

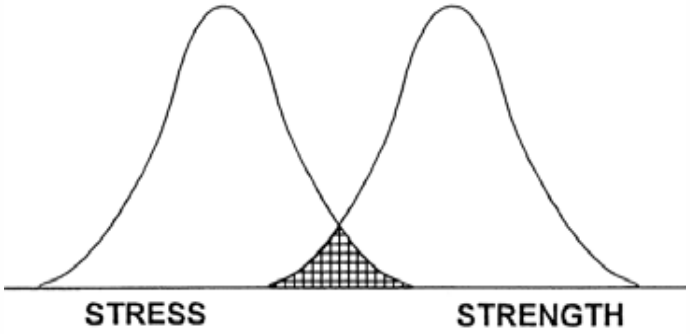


Stress-Strength Analysis.

Stress-Strength Interference.

- **Stress-Strength Overlap.**

  There is too much variability for the proximity of the means for stress and strength and there is an increased likelihood of failure which is represented by the overlapping shaded area.



Stress-Strength Analysis.

Stress-Strength Interference.

- **Modeling for Stress-Strength Overlap.**

  When the stress distribution and strength distribution are independent of each other,

$$\mu_{X-Y} = \mu_X - \mu_Y$$

$$\sigma_{X-Y} = \sqrt{\sigma_X^2 + \sigma_Y^2}$$

  To calculate the probability of a failure from stress-strength interference, the standard normal distribution and z tables are normally utilized.

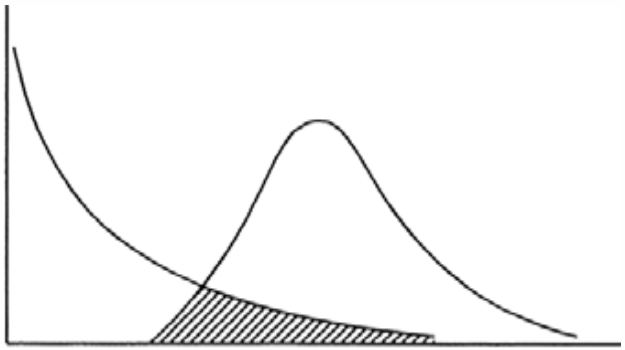
$$z = \frac{\mu_x - \mu_y}{\sqrt{\sigma_x^2 + \sigma_y^2}}$$

Stress-Strength Analysis.

Monte Carlo Simulation.

- Monte Carlo simulation is a technique that permits the setting up of a process to emulate real world conditions as closely as possible. In an area analysis, there may be several variable and distributions that are combined to determine the probability of a failure.

- The use of Monte Carlo simulations is greatly enhanced through the use of computers for generation random numbers and for analysis to determine if a significant event will occur.



FMECA.

[CRE Primer V 8-14]

Failure Mode and Effect Analysis (FMEA)

- This system examines ways in which a product or system failure may occur.
- FMEA starts with potential problems and looks for resulting bad effects.

Part No./Name: 37XT11-Lock Mech.
Project: Re-design
Other Departments: Shop Service, etc.
Subsystem Name: Quill Clamping Mechanisms
Suppliers Involved: Wilton and others
Design Responsibility: Bob Dovich

P = Probability
S = Seriousness
D = Likelihood
RPN = Risk Priority Number

FMECA No. 43
Final Design Deadline: Feb 1, 2003
Prepared By: RCD
Reviewed By: TRB
FMECA Date: 12-26-02
Rev.

PART NUMBER NAME	FUNCTION	POTENTIAL FAILURE MODE(S)	POTENTIAL EFFECT(S) OF FAILURE	POTENTIAL CAUSE(S) OF FAILURE	CURRENT CONTROLS	RISK ASSESSMENT				RECOMMENDED CORRECTIVE ACTION(S)	ACTION(S) TAKEN	REVISED RISK ASSESSMENT				RESPONSIBLE DEPT OR INDIVIDUAL
						P	S	D	RPN			P	S	D	RPN	
WILTON POWER LOCK	CLAMP	LEAK	HOUSE-KEEPING	WEAR	ACCEPT SUPPLIER'S INFO	2	4	3	24	DISCUSS WITH SUPPLIER						
		LOSES CLAMPING FORCE (SHIFTING)	MACHINING PARTS OVERSIZE	SELECTED INADEQUATE SIZE POWER LOCK	ENG. STANDARD	2	4	4	32	PERFORM LOAD TESTS						
				MATERIALS & WORKMAN-SHIP	STD. Q.C.	1	4	2	8	NONE						
				OVER PRESSURE	NONE	2	4	2	16	REVIEW NEED FOR SYSTEM TO PREVENT OVER-PRESSURIZATION						
				PUMP SIZING	ENG. STANDARD	1	4	2	8	REVIEW PRESSURE DELIVERED IN FIELD AND ACTUAL NEED.						

FMECA.

[CRE Primer Ⅴ 8-14]

Failure Mechanisms vs. Modes.

- **Failure Mode.**

  The failure mode is the actual symptom of the failure. That is, the failure mode may be "premature engine shut-down," or "70% degradation of function," or any other description of what external occurrence will be defined as a failure.

- **Failure Mechanisms.**

  Failure mechanisms are the individual, or multiple reasons that cause the failure mode. For instance, a failure mechanisms might be "corrosion," or "contamination," or any other description of reasons that might cause a failure mode.

FMECA.

[CRE Primer Ⅴ 8-14]

Risk Assessment.

- Risk assessment is the combination of the probability of an event or failure and the consequence(s) of that event of failure to a system's operators, users, or its environment.

- The analysis of risk of failure normally utilizes two measures.
  1. Severity of failure.
     The effect of the failure on the system, operators, or mission.
  2. Probability of failure.
     The likelihood of the failure occurring.

FMECA.

[CRE Primer Ⅴ 8-14]

The severity of failure.

· Hazard Severity Categories : MIL-STD-1629A.

	Classification	Description
Ⅰ	Catastrophic	A failure that may cause death or mission loss
Ⅱ	Critical	A failure that may cause severe injury or major system damage.
Ⅲ	Marginal	A failure that may cause minor injury or degradation in mission performance.
Ⅳ	Minor	A failure that does not cause injury or system damage but result in system failure and unscheduled maintenance.

FMECA.

[CRE Primer V 8-14]

The Probability of Failure.

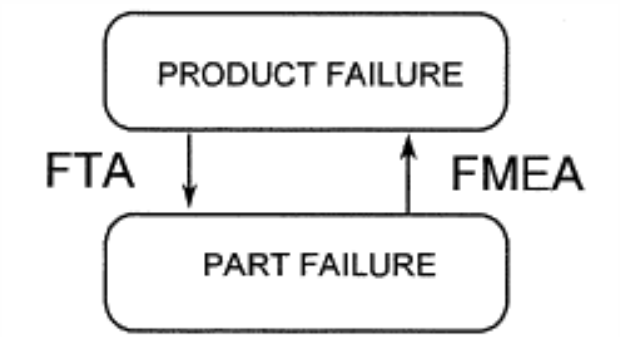
· Common Failure Probability Ranking.

Failure Probability Level	Description	Example
A	High likelihood of occurrence	> 10^{-1}
B	Probable occurrence.	10^{-1} to 10^{-2}
C	Occasionally occurs.	10^{-2} to 10^{-3}
D	Remote probability.	10^{-3} to 10^{-6}
E	Highly unlikely.	< 10^{-6}

FTA.

Fault Tree Analysis.

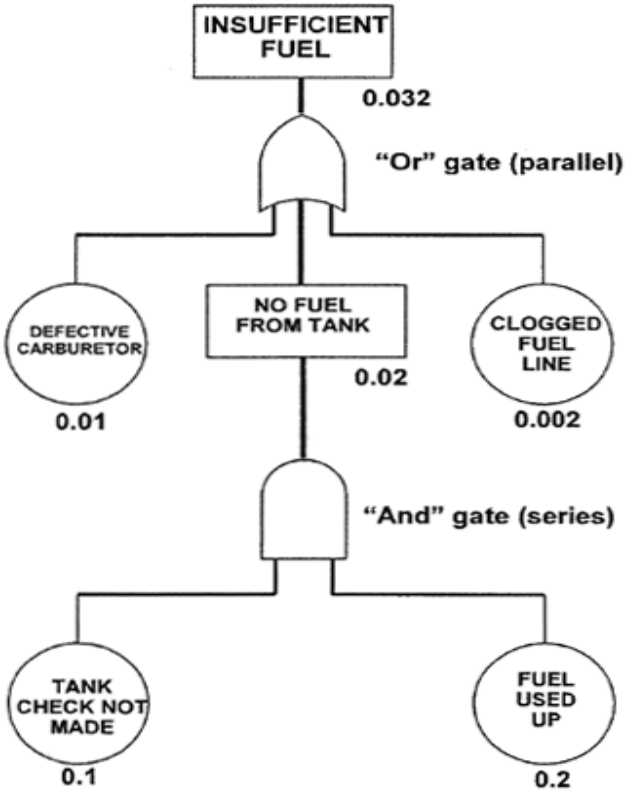
- In contrast to FMEA, that predicts product failure from part failure, FTA is used to identify parts responsible for product failure. FMEA is a qualitative analytical technique, whereas FTA can be a quantitative techniques.



FTA.

Fault Tree Analysis.

- FTA starts with undesired events for which the designer must provide some solution. Safety hazards and injuries are often diagnosed with this method.



Tolerance and Worst Case Analysis.

[CRE Primer V 16-18]

Worst Case Analysis.

- Another method of evaluating the design reliability is to analyze the design assumption the worst case. That is, assuming that the components are at the extreme in tolerance, environmental or operating conditions.

- The worst case may be evaluating using one of three methods : Root Sum Squared, Extreme Value, or Monte Carlo.

- **Random variation vs. Bias variation.**
  - Random variation are variation that are not predictable.
  - Bias variation are variation that are known to occur as the result of an environmental or time effect and are predictable in their direction and amount.

Tolerance and Worst Case Analysis.

[CRE Primer V 16-18]

Root-Sum-Square Analysis (RSS).

- RSS uses the statistical nature of the random variation of components to compute their contribution. The random effects are added as the square root of the sum of the squares of the expected variation.

- **Worst Cases Length Maximum.**

  $\sum$ (Normal Lengths) + $\sqrt{\sum(3\sigma)^2}$ + $\sum$ (Length Increase Due to Environmental Factors)

Tolerance and Worst Case Analysis.

[CRE Primer V 16-18]

Extreme Value Method (EVA).

- The most conservative method of determined worst case is the extreme value method (EVA). In this method the contribution by the random effects are added algebraically rather that as the root-sum-squared.

- **Worst Cases Length Maximum.**

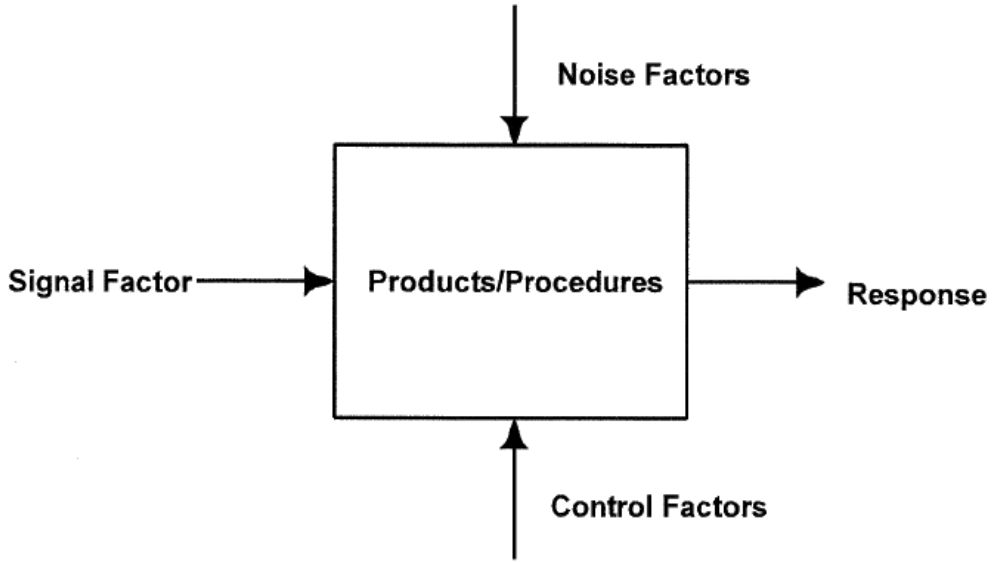
  $\sum$ (Normal Lengths) + $\sum(3\sigma)$ + $\sum$ (Length Increase Due to Environmental Factors)

Robust Design.

The Robust Design Approach.

- The appropriate use of robust design approaches is a process that can produce extremely reliable designs both during manufacturing and in use.

- Robust design uses parameter control to place the design in a position where random "noise" does not cause failure.



Robust Design.

[CRE Primer V 19-34]

The Robust Design Approach.

- **Signal factors.**
  - The factors that strongly influence the mean response.
  - Signal factors normally have minimal influence in varying the output response and are controllable.

- **Noise factors.**
  - The factors that influence the variation in the output.
  - These may be controllable or non-controllable.
  - The controllable ones are varied during the experimentation to see which combination gives the highest signal to noise ratio(S/N). In essence, choose the levels of controllable noise factors such that the S/N ratio is maximized and the output response is insensitive to the variation in uncontrollable noise factors.

Robust Design.

[CRE Primer V 19-34]

The Robust Design Approach.

- **Concept design**.

  The selection of parts, methods, and tentative product parameter values.

- **Tolerance design**.

  The establishment of the permissible variation in the product and process to achieve a consistent output.

- **Parameter design**.

  The selection of nominal product and process operating levels, to determine the optimum combinations.

Robust Design.

[CRE Primer V 19-34]

Concept Design.

- Concept design (also called system design) is the selection of the process or product architecture based on technology, costs, customer requirements, or other important considerations.

- Two objectives of concept design.
  - Develop a product that can perform the desired functions and be robust under various operating or exposure conditions.
  - Have the product manufactured at the lowest possible cost.

Robust Design.

[CRE Primer V 19-34]

Parameter Design.

- Parameter designs improve the functional robustness of the process so that the desired dimensions or quality characteristics are obtained.

- **Parameter design process.**
  1. Determine the signal factors and the uncontrollable noise factors and ranges.
  2. Choose as many controllable factors as possible, select levels for these factors, and assign these levels to appropriate orthogonal arrays.
  3. Calculate S/N ratios

$$\eta = \frac{S}{N} = 10\log\frac{1}{r}\left(\frac{s_\beta - V_e}{V_N}\right)$$

  4. Determine the optimal conditions for the process.
  5. Conduct actual production runs.

Robust Design.

[CRE Primer V 19-34]

Signal-to-Noise Ratio.

- S/N ratio is a calculation to quantify the effects of variation in the controllable factors resulting in the variation of output.

- Smaller is better. S/N (in dB) = -10 LOG $\frac{1}{n}\left(\frac{1}{(Y_1)^2}+\frac{1}{(Y_2)^2}+\cdots+\frac{1}{(Y_n)^2}\right)$

- Larger is better. S/N (in dB) = -10 LOG $\frac{1}{n}\left((Y_1)^2+(Y_2)^2+\cdots+(Y_n)^2\right)$

- Nominal is best. S/N (in dB) = -10 LOG $\frac{y^2}{s^2}$

where n : The number of observations of controllable factors with experimentation.

Y : The output response for each experiment conducted.

y : Mean s^2 : Variance.

Robust Design.

[CRE Primer V 19-34]

Example Orthogonal Design Layout.

L_8 ARRAY

	8	7	6	5	4	3	2	1	#
	2	2	2	2	1	1	1	1	E
	2	2	1	1	2	2	1	1	F
	1	1	2	2	2	2	1	1	E x F
	2	1	2	1	2	1	2	1	G
	1	2	1	2	2	1	2	1	E x G
	1	2	2	1	1	2	2	1	F x G
	2	1	1	2	1	2	2	1	E x F x G
	120h	120h	120h	120h	24h	24h	24h	24h	(E) Time
	150F	150F	72F	72F	150F	150F	72F	72F	(F) Temp
	75%	25%	75%	25%	75%	25%	75%	75%	(G) R. H.

L_9 ARRAY

	#	A	B	C	D	Inter-ference (A)	Wall Thickness (B)	Ins. Depth (C)	Percent Adhesive (D)	Response								Avg.	S/N RATIO (db)
Experimental Conditions	1	1	1	1	1	Low	Thin	Shallow	Low	19.1	20.0	19.6	19.6	19.9	16.9	9.5	15.6	17.5	24.025
	2	1	2	2	2	Low	Medium	Medium	Medium	21.9	24.2	19.8	19.7	19.6	19.4	16.2	15.0	19.5	25.522
	3	1	3	3	3	Low	Thick	Deep	High	20.4	23.3	18.2	22.6	15.6	19.1	16.7	16.3	19.0	25.335
	4	2	1	2	3	Medium	Thin	Medium	High	24.7	23.2	18.9	21.0	18.6	18.9	17.4	18.3	20.1	25.904
	5	2	2	3	1	Medium	Medium	Deep	Low	25.3	27.5	21.4	25.6	25.1	19.4	18.6	19.7	22.8	26.908
	6	2	3	1	2	Medium	Thick	Shallow	Medium	24.7	22.5	19.6	14.7	19.8	20.0	16.3	16.2	19.2	25.326
	7	3	1	3	2	High	Thin	Deep	Medium	21.6	24.3	18.6	16.8	23.6	18.4	19.1	16.4	19.9	25.711
	8	3	2	1	3	High	Medium	Shallow	High	24.4	23.2	19.6	17.8	16.8	15.1	15.6	14.2	18.3	24.833
	9	3	3	2	1	High	Thick	Medium	Low	28.6	22.6	22.7	23.1	17.3	19.3	19.9	16.1	21.2	26.152

Robust Design.

[CRE Primer V 19-34]

Tolerance Design.

- Quality loss function indicates a loss of society. The use of the loss function illustrates that there is value in reducing variation in the product.

$$L(y) = k(y - m)^2$$

- The tolerance for all system components must be determined. This includes the types of material used. In tolerance design, there is a balance between a given quality level and cost of the design. The measurement criteria is quality losses.

Robust Design.

[CRE Primer V 19-34]

Tolerance Design.

- Quality losses are estimated by the functional deviation of the products from their target values plus the quality losses.

$$L(y) = k(y-m)^2$$

$$k = \frac{\text{cost of a defective product}}{(\text{tolerance})^2} = \frac{A_0}{\triangle^2}$$

$$\triangle = \frac{\triangle_0}{\Phi}, \qquad \Phi = \sqrt{\frac{A_0}{A}}$$

where, Φ = The economical safety factor.

$\triangle_0$ = Functional limits

$\triangle$ = Tolerance specification.

Robust Design.

[CRE Primer V 19-34]

Taguchi's Quality Imperatives.

- Robustness is a function of product design. The manufacturing process and on-line quality control cannot do much to change that.

- Robust products have a strong signal with low internal noise. Increasing the signal-to-noise ratio will improve the robustness of the product.

- For new products, use planned experiments that vary values, stresses, and conditions to seek out the parameter targets. Orthogonal arrays are recommended.

- To build robust products, simulate customer-use conditions.

- Tolerances are set before going to manufacturing.

Robust Design.

[CRE Primer Ⅴ 19-34]

Taguchi's Quality Imperatives.

- The quality loss function can be measured.

- Product that barely meet the standard are only slightly better that products that fail the specifications. The aim is for the target value.

- The factory must manufacture products that are consistent. Reduced variation is needed for consistency.

- Reducing product variation in the factory will reduce the number of defectives in the field. A reduction in part variation will decrease system variation.

- Proposals for capital equipment for on-line quality effects should have the average quality loss added to the proposal.

Human Factors in Reliability.

[CRE Primer V 36-38]

Design for Human Factors.

- In many product design development projects, the integration of people into the hardware and software segments is the most challenging. The human element performance is often a key component of mission or project success.

- Human factors must be considered in any product design. The consideration may be broken down into the three categories.
    1. Safety.
    2. Workmanship.
    3. Maintainability.

Human Factors in Reliability.

[CRE Primer V 36-38]

Safety.

- Safety considerations are obviously of paramount concern in any design. Any safety consideration should be considered critical and of top priority.

- Safety considerations should include not only the expected use of the product, but also the unexpected use. Human beings are famous for not following instructions. Therefore, safety considerations should ultimately conclude with "fail-safe" features that protect us from ourselves.

Human Factors in Reliability.

[CRE Primer V 36-38]

Workmanship.

- Workmanship during manufacturing 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.

Maintainability.

- Maintainability is another human factor concern in that the device should e maintainable easily by the operators. There are many examples of poor reliability that can be traced to poor maintenance. The designers is not responsible to perform the maintenance, but is responsible to include maintenance considerations.

Human Factors in Reliability.

[CRE Primer V 36-38]

Some human-machine design principles.

- **Standardization.**

  Can the product be made or operated easier if key components are standardized to similar or known products ?

- **Automation.**

  Can boring, tiring or complex operations be automated with suitable hardware/software replacements ?

- **Simplification.**

  What can be done to streamline the design ? Will fewer controls displays or job aids assist human performance ?

Human Factors in Reliability.

[CRE Primer V 36-38]

Some human-machine design principles.

- **Load Sharing.**

  Can any physical and psychological human tasks be abated ? Consideration including jab sharing, job rotation, design simplification and/or machine replacement.

- **Sensory Amplification.**

  What can be altered about the design to assist human performance, considering age, weight, height, hearing, sight and dexterity ?

DFX

[CRE Primer Ⅴ 39-46]

Design for X.

- Design for X(DFX) is defined as a knowledged-based approach for designing products to have as many desirable characteristics as possible.

- The desirable characteristics include : Quality, Reliability, Testability, Assembly, Manufacturability, Environment, Serviceability (Maintainability and Repairability), Safety, User friendliness, Appearance, Packaging, Feature, Time to Market.

DFX

[CRE Primer Ⅴ 39-46]

Design for Quality : QFD.

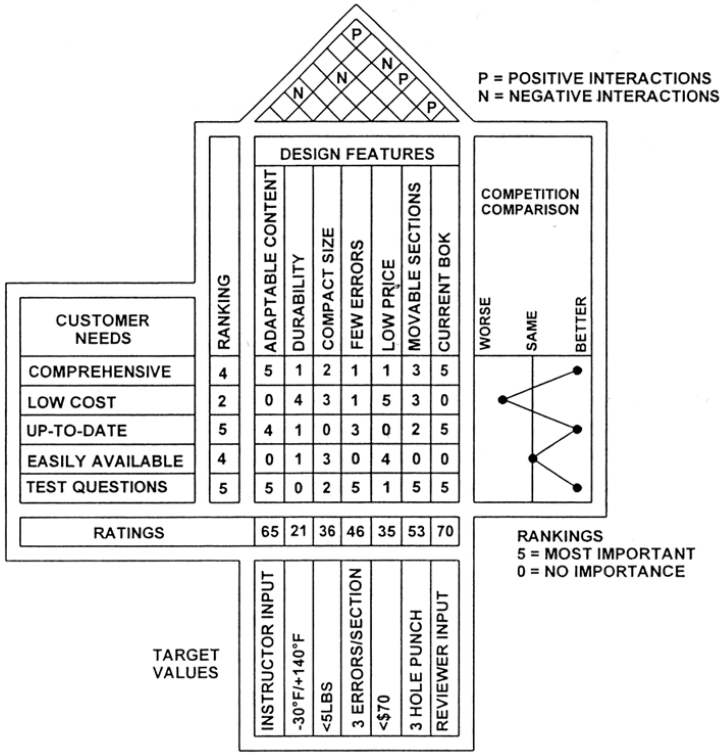
- Quality function deployment is a tool that is sometimes referred to as the "voice of the customer", or as the "house of quality".
- QFD has been described as a process to ensure that customers' wants and needs are heard and translated into technical characteristics.
- The technical characteristics are handled through a cross functional team that includes sales, marketing, design engineering, manufacturing engineering, and operation.

DFX

[CRE Primer V 39-46]

Benefits of QFD.

- The possible benefits for using the QFD process.
  1. Creates a customer driven environment.
  2. Reduces the cycle time for new products
  3. Uses concurrent engineering methods.
  4. Reduces design to manufacture costs.
  5. Increases communication through cross functional teams.
  6. Creates data for proper documentation of engineering knowledge.
  7. Establishes priority requirements and improves quality.



Part and System Management.

[CRE Primer V 47-51]

Areas of Part and System Management.

- Part Selection.
- Materials Selection and Control.
- Derating Methods and Principles.
- Establishing Specification.

Part Selection.

[CRE Primer Ⅴ 47-51]

Some Consideration for Part Selection.

- Selection of obsolete (or soon to be) and sole sourced parts and materials.
- Possibility of diminishing sources.
- Use of unproven or exotic technology.
- Incompatibility with the manufacturing process.
- Inventory volume expansion and increase in cost.
- Supplier quality may be difficult to monitor due to the added number of suppliers.
- Loss of "ship-to-stock" or "just-in-time" purchase opportunities.
- Limited ability to benefit from volume buys.
- Additional tooling and assembly methods may be required to account for the added variation in part characteristics.
- Part reliability can decrease due to the uncertainty and lack of experience with new part.
- Automation efforts may be impeded due to the number of additional part types.

Part Specification.

[CRE Primer V 47-51]

ER Electrical Components.

- Military established reliability (ER) components provide the minimum known levels of reliability (maximum failure rates) demonstrated under controlled test conditions.

MIL Symbol	Failures/10^6 hours
L	2000
M	1000
P	100
R	10
S	1
T	0.1

- Components procured to ER specifications are subjected to special process controls, lot acceptance testing, screening, and extended life tests. Level P or better is recommended for military equipment.

Part Specification.

[CRE Primer V 47-51]

JAN, JANTX and JANTXV.

- Military grade, high reliability semiconductors are procured to MIL-S-19500.

- JAN is the minimum level of MIL-S-19500. "TX" indicates JAN processing plus "testing extra" referring to special process and power conditioning on a 100% basis. "TXV" devices pass all JAN and TX requirements plus an internal, visual precap inspection.

- The relative failure rates for JAN, JANTX, and JANTXV are 1.0, 0.2 and 0.1 (per 10^6 hours) respectively.

Derating.

[CRE Primer Ⅴ 54-56]

Definition of Derating.

- Using an item in such a way that applied stresses are below rated values, or

- The lowering of the rating of an item in one stress field to allow an increase in rating in another stress filed.

Derating.

[CRE Primer V 54-56]

Stresses an Item is Subjected.

- **Environmental stress.**

  Temperature, Humidity, Contamination, Vibration and other conditions that act on a component.

- **Operational stress.**

  Voltage, Current, Flow, Amplitude, Dynamic loading and other stresses that manifest themselves during operation.

Derating.

[CRE Primer V 54-56]

Safety Factor.

- Safety Factor : $\frac{\mu_x}{\mu_y}$
- Margin of Safety : $\frac{\mu_y - \mu_x}{\mu_y}$

where μ_x = average strength and μ_y = average stress or load

Derating.

[CRE Primer V 54-56]

Examples of Part Derating Values.

Part Type	Derating Parameter	Environment	
		Severe	Benign
Capacitors	DC Voltage Temp from Max Limit	60% 10°C	90% NA
Diodes	Power Dissipation Max Junction Temp	70% 125°C	90% NA
Lamps	Voltage	94%	94%
Microcircuit	Supply Voltage Fan Out Max Junction Temp	±5% 80% 125°C	±5% 90% NA
Microprocessors	Supply Voltage Fan Out Max Junction Temp	±5% 80% 125°C	±5% 90% NA
Resistors	Power Dissipation Temp from Max Limit	50% 30°C	80% NA

Reliability Specifications.

[CRE Primer V 60-61]

Establishing Reliability Specifications.

- Mean Time Between Failure (MTBF) or Mean Time To Failure (MTTF).

- Mean Time Between Maintenance (MTBM)

- Availability.
  Availability is a combination of MTBF, MTBM, and average maintenance time.

- Failure-Free Period of Operation.

- Service Life.
  Service life is frequently applied to structures such as bridges, where fatigue and wear-out are the principal failure modes.

Reliability Specifications.

[CRE Primer Ⅴ 60-61]

Establishing Reliability Specifications.

- Damage Tolerance.

  A damage tolerant design is one in which individual components may fail without failure of total device. Another concept of damage tolerance is that the structure will function long after a component failure is easily detectable.

- No Single Point Failure.

  This reliability requirement specifies that no single item or failure mode will cause total failure of the system.

- Fail-safe.

  Fail-safe means that the device will fail in a safe state. For instance, early elevator construction was risky until devices were developed that prevented the elevator from falling if the cable or drive motors failed.

Reliability Specifications.

[CRE Primer V 60-61]

Establishing Reliability Specifications.

- Graceful Failure.

  Graceful failure means that the failure should be acceptable to the customer (at least as acceptable as any failure can be). For instance, software failure that allow the user to continue with the program are graceful.