Reliable Design: Basic Approach

Jiří Stodola[1] and Jan Furch[2]

[1]*University of Defence, Faculty of Military Technology, Kounicova 65, 662 10 Brno, Czech Republic*
[2]*University of Defence, Faculty of Military Technology, Kounicova 65, 662 10 Brno, Czech Republic*

Abstract. The knowledge and experience learnt from product designing have resulted in development of their reliability theory. The classical concept of safe – life is based on product over dimensioned design that considers safety factor or safety margin for measure. However, practical engineering has found this concept in a manner inconvenient as design fault-resistance to determine the ultimate condition and operating stress are random values. A way out is in the concept of stochastic approach to reliability design resulting from the defect-production probability distribution law. That concept allows product designing with predetermined reliability, such as in the example contained in this paper.

1 Introduction

You may question first how reliability has anything to do with design, but it's one of the most important aspects of design. There are undoubtedly objective principles about designing reflected in both the creative procedure and possible algorithmization or automation of each of the processes. Algorithmization then stands for a general procedure of multiple steps leading to the result of the questioned task. Algorithmization of designing is a systematic method possibly completed for practical effect with intuitive methods using the designer's or the creative individual's education, knowledge and experience bases for the results. The systematic and intuitive kind methods do complete rather than inhibit from each other that make us think of a new design discipline – Design Science. The first phase of a new equipment design project is dimensioning process of setting up the mechanical parts size supporting cross-section dimensions so that they stand the external load. It is practical a priori determination on design requirements of strength, rigidity and other features that include also reliability at reasonable production cost. The current practice in designing has determined the essential parameters and functions to assess the load strength of the material by modelling single-value deterministic variables [1]. The errors of calculation, if any, material defects, inaccurate knowledge of loading forces, oscillating load cycles and others are considered within the safety factor "k". The stress-restricted designs have the acceptance criterion in the following form:

$$S \geq s \cdot k, \tag{1}$$

where $k > 1$ for the safety factor. However, safety induced in such a way to the design misses information of the construction element failure option in the form of failure probability *F(t)*. This conventional attitude supposes that sufficiently high safety factor k may completely eliminate the failure possibility. However, most design variables are actually random values that temper with the probability theory and mathematic statistics principles [2]. Therefore, the failure probability *F(t)* may vary a lot depending on element load and strength random variables distribution at equal safety factor k. Should the machine constructions design reflect their reliability the design formulas should consider stochastic character of all the variables and use all the terms for the general design. This attitude to designing called reliability (probability) design has developed only recently. Its suitability for aircraft or automotive industries has increased as reliability of the product, such as aircraft or automobile has become an important factor besides economic operation in the competitive environment of the global market.

2 Conventional and reliability based approach to construction design

The reliability of product is strongly influenced by decisions made during the design process. Deficiencies in design affect all items produced and are progressively more expensive to correct as development proceeds. It is often not practicable or economic to change a design once production has started. It is therefore essential that design disciplines are used which minimize the possibility of failure and which allow design deficiencies to be detected and corrected as early as possible. The design process must therefore be organized to ensure that failure-free design principles are used and that any deviations from the principles are detected and corrected.

Failure-free design is the only acceptable principle for any reliability-conscious project team. Anything less will to be reflected in the acceptance of failures throughout the development and production cycle, and a low rate of improvement. The designer must produce designs which will not fail in manufactured and used as specified. In order to be able to do this test data may be needed to reduce uncertainties. Any subsequent failures can then be firmly classified as design deficiencies which escaped the review or test system, or as being due to manufacturing failures or overload. Failure-free design therefore involves prevention, check and cure. The designer must be aware of the materials, processes, components, production methods, design rules and guidelines, costs, and much else in order to create a good design.

Computer-aided engineering (CAE) methods are available to assist with a wide variety of design tasks. Their power, ease of use, and increasing availability due to reducing costs of computing equipment and software are resulting in increasing applications. CAE is also makes possible the creation of designs which would otherwise be very difficult or uneconomic, for example complex electronic circuits. CAE can also provide enormous improvements in engineering productivity. In the mechanical engineering field, software is available for stress analysis, which performs finite element analysis calculations for mechanical and thermal stress calculations, and for analysis of vibration and load responses. Drafting software is used for generating manufacturing drawings and machine tool instructions, and this can also be used to optimize the design of mechanisms. Specialist CAE software is also available for design and analysis of systems and products incorporating other technologies, such as hydraulics, magnetics, microwave electronic, etc. Multi-technology capability is now also being provided, so that mixed technology designs can be modelled and analysed. CAE provides the capability for rapid assessment different design options, and for analysing the effects of tolerances, variation, and failure modes. Therefore if used in systematic, disciplined way, with adequate documentation of the options studied and assessments performed, designs can be optimized for costs, and reliability. CAE should be considered as a powerful aid to more cost-effective and correct design, not merely a means of speeding up the design process. However, there are important limitations inherent in most CAE tools. The software models can never be totally accurate representations of all aspects of the design and of its operating environment. For example, electronic circuit simulation programs generally ignore the effects of electromagnetic interference between components, and drafting systems will ignore distortion due the stress of temperature. Therefore it is essential that engineers using CAE are aware of the limitations, and how these could affect their designs. The effective application of modern CAE places greater responsibility upon designers to be aware of the practical aspects and limitations of the relevant technologies. Otherwise they can be easily misled into placing undue faith in the accuracy and completeness of the software models, resulting in incorrect or unreliable designs.

The environments in which the product will be expected to be stored, operated and maintained must be carefully assessed, as well as the expected severity and durations. The assessment must include all aspects that could affect the product ́s operation, safety and reliability. Physical factors include temperature, vibration, shock, humidity, pressure, etc. Extreme values and, where relevant, rotes of change must be considered. Other environmental conditions, such as corrosive atmospheres, electrical interference, power supply variation, etc., must also be taken into account. Where appropriate, combined environmental conditions, such as temperature, corrosive atmosphere and vibration, contamination, should be assessed. An aspect of the environment often neglected is the treatment of the product by the people in storage, handling, operation and maintenance. Environmental aspects should be reviewed systematically, and the review should be properly documented. The protective measures to be taken must be identified, as appropriate to storage, transport, handling, operation and maintenance. Protective measures include packing, provision of warning labels and instructions, protective treatment of surfaces, and design features.

Protections against extreme loads is not always possible, but should be considered whenever practicable. In many cases the maximum load can be predetermined, and no special protection is necessary. However, in many other loading situations extreme external loads can occur and can be protected against. Standard products are available to provide protection against, for example, overpressure in hydraulic or pneumatic systems, impact loads or electrical overload. When overload protection is provided, the reliability analysis is performed on the basis of the maximum load which can be anticipated, bearing in mind the tolerances of the protection system. In appropriate cases, loads which can occur when the protection system fails must also be considered. However, in most practical cases it will be sufficient to design to withstand a predetermined load and to accept the fact that loads above this will cause failure. The probability of such loads occurring must be determined for a full reliability analysis to be performed. It may not always be practicable to determine the distribution of such extreme events, but data may be available either from failure records of similar items, or form test or other records. Where credible data are not available, the worst design load case must be estimated. The important point is that the worst design case is estimated and specified. A common cause of failure is the use of safety factors related to average load conditions, without adequate consideration having been given to the extreme conditions which can occur during use of the product.

Strength degradation, it is many forms, can be one of the most difficult aspect to take into account in design reliability analysis. Strength degradation due to fatigue in materials is fairly well understood and documented, and therefore reliability analysis involving metal fatigue, including the effects of stress raisers such as notches, corners, holes and surface finish, can be performed satisfactory, and parts can be designed to operate below the fatigue limit, or for a defined safe life. However, other weakening mechanisms are often more complex. Combined stresses may accelerate damage or reduce the fatigue limit. Corrosion and wear are dependent upon environments and lubrication, the effect of which is therefore often difficult to forecast. If complete protection is not possible, the designer must specify maintenance procedures for inspection, lubrication or scheduled replacement. Reliability analysis of designs with complex weakening processes is often impracticable. Test should then be designed to provide the required data by generating failures under known loading conditions.

Despites discipline, training and care, it is available that occasional oversights or errors will occur in new designs. Design analysis methods have been developed to highlight critical aspects and to focus attention on possible shortfalls. Design analyses are sometimes considered tedious expensive. In most cases the analysis will show that nearly all aspects of the design are satisfactory, and much more effect will have been expended in showing this than in highlighting a few deficiencies. However, the discovery of a very few deficiencies at an appropriately early stage can save far more than the cost that might be incurred by having to modify the design at a later stage, or by having to live with the consequences of the defect. Therefore, well-managed design analyses are extremely cost-effective. The tedium and expense can be greatly reduced by good planning and preparation and by the use of computerized methods. The main reliability design analysis techniques are:

1. Quality function deployment (QFD).
2. Load-strength analysis (LSA).
3. Reliability prediction.
4. Hazard and operability study (HAZOPS.
5. Fault tree analysis.
6. Failure modes, effects and critically analysis (FMEA, FMECA, etc.).
7. Parts materials and process review (PMP).
8. Human aspects manufacturing.
9. Aspect of maintenance.
10. Others.

For example, load-strength analysis (LSA) is a procedure to ensure that all load and strength aspects have been considered in driving the design, and if necessary in planning of tests. The load-strength analysis should include the following:

- determine the most likely worst case values and patterns of variation of load and strength,
- evaluate the safety margin for intrinsic reliability,
- determine protection methods (load limit, derating, screening, other quality control methods),
- identify and analyse strength degradation modes,
- test to failure to corroborate, analyse results,
- Correct or control (redesign, safe life, quality control, maintenance etc.).

This part of the text is taken from [3]. The book [3] contains summary information including the use of reliability theory in practice, not only for designers but also for users.

Reliability designing is based on the presumption the design variables are random values [4], [5]. Their variability rate may be used for attaining the required construction reliability. The difference of the reliability-based and conventional (deterministic) design [6] may be explained on the design example of strength S intended to transmit static service load s. The conventional approach to design introduces safety factor $k > 1$ and according to the equation (1) the design criterion takes the following form:

$$\frac{S}{S_{max}} = k \qquad (2)$$

where S - characteristic material strength (such as yield point, ultimate strength, endurance limit and others), S_{max} - maximum permissible stress (such as tension etc.) [7].

The actual operating stress must comply the following condition:

$$s \leq s_{max} = \frac{S}{k} \rightarrow S - s \geq k, \qquad (3)$$

to guarantee failure is avoided. Failure occurrence probability cannot be reflected in the formula or specify with a value [8]. The reliability design approach reflects reliability or design safety in the form of failure-proof probability. The design criterion is considered in the following form:

$$S > s \rightarrow (S - s) > 0\,. \qquad (4)$$

Probability introduced to the in equation results in the following:

$$P(S > s) =\rightarrow (S - s) = R\,, \qquad (5)$$

where $S = (\widehat{S}, \sigma_S$ characteristic material strength, $s = (\widehat{s}, \sigma_s)$ maximum accessible operating stress, P - probability of failure-proof operation, i.e. structural reliability.

The equation (5) may be expressed in words that due to probability R material strength is higher than the acting tension caused by the operating load and prevents the failure [9]. The difference of the conventional and reliability approaches is characterised in figures 1 and 2 [2], [10], [11], [12].

3 Reliability designing and analysis

If part strength $S = (\mu_S,\ \sigma_S^2)$ considered when the random values are distributed along normal (Gauss) rule $N(\mu,\ \sigma^2)$ where $\mu,\ \sigma^2$ are real numbers, $\sigma^2 > 0$ thus

$$f(S) = \frac{1}{\sigma_S\sqrt{2\pi}} \exp - \frac{(S-\mu_{S)}}{2\sigma_S^2} \qquad (6)$$

while $S \in (\pm\infty)$, or $(-\infty < S < \infty)$. This part is randomly loaded with stress $s = (\mu_s,\ \sigma_s^2)$ with normal distribution, then

$$f(s) = \frac{1}{\sigma_S\sqrt{2\pi}}\exp - \frac{(s-\mu_S)}{2\sigma_S^2} \tag{7}$$

and $(-\infty < s < \infty)$.

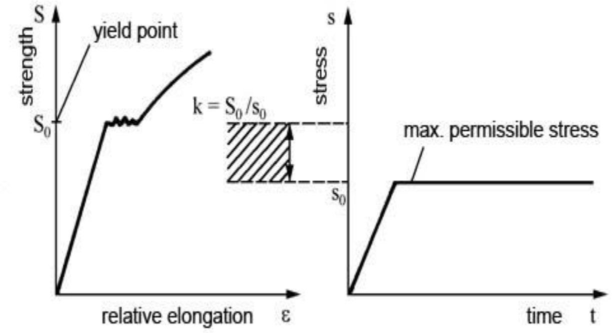

Figure 1. Conventional design

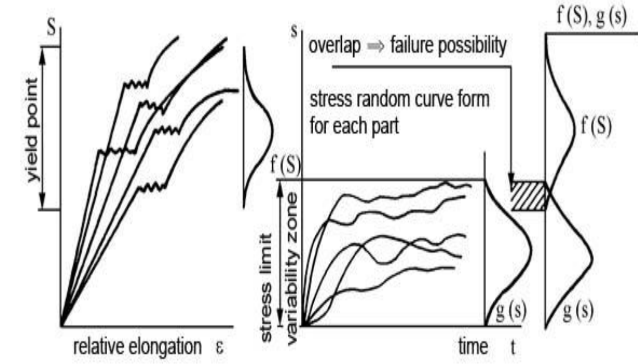
S
yield point
relative elongation ε
s
overlap ⇒ failure possibility
stress random curve form for each part
f (S)
stress limit variability zone
time t
g (s)
f (S), g (s)
f (S)
g (s)

Figure 2. Reliability design

Equation (5) implies $R = P(S - s > 0)$ and the difference is $z = S - s$ with the following characteristics:

$$\mu_z = \mu_S - \mu_s \tag{8}$$

and

$$\sigma_z = \sqrt{\sigma_S^2 - \sigma_s^2} \tag{9}$$

then

$$R = \frac{1}{\sigma_z\sqrt{2\pi}}\int_0^\infty exp - \frac{(z-\mu_z)}{2\sigma_z^2}dz\,. \tag{10}$$

This equation is used in the form of standard (basic) normal distribution utilising the known transformation

$$t = \frac{z-\mu_z}{\sigma_z} \tag{11}$$

that implies the following for the variable t limits: $z = \infty \rightarrow t = \infty$ and $z = 0 \rightarrow t = \frac{\mu_z}{\sigma_z}$.

$$R = \frac{1}{\sqrt{2\pi}}\int_{\mu_Z/\sigma_Z}^{\infty} exp\frac{t^2}{2}\mathrm{dt} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\mu_Z/\sigma_Z}\frac{\mu_Z}{\sigma_Z} = \Phi(\frac{\mu_Z}{\sigma_Z}). \tag{12}$$

The upper limit value of t is determined as follows

$$t = \frac{\mu_Z}{\sigma_Z} = \frac{\mu_S-\mu_S}{\sqrt{\sigma_S^2-\sigma_S^2}}. \tag{13}$$

The equation (12) is the distribution function of the standard random variable *Φ(t)* with normal distribution $N = (0, 1)$. The values of the standard random variable t distribution function variable *Φ(t)* are called Laplace's functions (probability integral) being tabled in e.g. [13], [14], [15]. There are two general approaches to the reliability calculation:

1) For the already produced and used constructions, substitution of the known values of μ_S, σ_S and $\mu_s,\ \sigma_s$ in the equation (13) determines the upper limit value of t for the analysed construction and with the standard normal distribution $N = (0, 1)$ tables [14], [16], [17] specify the questioned construction's reliability. The following analysis example shows the procedure: An automobile constructional part is loaded with static stress of normal distribution $N(\mu_s = 135\ \text{MPa and}\ \sigma_s = 11.6\ \text{MPa})$ and its strength is $N(\mu_S = 184\ \text{MPa and}\ \sigma_S = 21.5\ \text{MPa})$. The task is determination of the part defect probability. The equations (8), (9) and (11) imply: $\mu_z = \mu_S - \mu_s = 184 - 135 = 49$; $\sigma_z = \sqrt{(21.5)^2 + (11.6)^2} = 24.4$ then $t = 49/24.4. = 2$ and the standard normal distribution function tables [14] show that the automobile part reliability $R(t) = 0.9773$ and failure probability $F(t) = 1 - R(t) = 0.0227$.

2) The design of new parts issues from the prior requirement of reliability R of the structure. When the required *to* value is known, the constructional variables are set so that the required reliability is achieved. This procedure is the basic tool for designing parts of in-advance-determined reliability [18], [19], which is the principal purpose of mechanical parts reliability designing. The following is an example of the procedure.

Remark: The examples include only static stress with forces constant in time to make calculation easy and clear. However, practical calculations should consider mostly forces variable in time – deterministic (load-time history is determined by function that can be mathematically described, such as cyclic – symmetric, discontinuous, pulsating, asymmetrical or others) and stochastic (random) that cannot be described exactly by mathematics but using rather statistic assessment.

A simple automobile constructional part (rod) is only loaded with static axial load Q of normal distribution $N\big(\mu_Q = 12.7 \cdot 10^4\text{N and}\ \sigma_Q = 1.8 \cdot 10^4\ \text{N}\big)$. The rod is made from steel with the yield point in tension normally distributed $N(\mu_x = 350\ \text{MPa and}\ \sigma_x = 35\ \text{MPa})$. The design requires failure probability $F(t) = 10^{-5}$, i.e. $R(t) = 0.99999$. The rod is made in an automatic production process where the resulting rod cross-section A is known to be a random variable of the coefficient of variation $v_A = 0.05$, which implies the mean-root-square error $\sigma_A = 0.05\,\mu_A$. The designer is now to calculate the minimum nominal cross-section of the rod μ_A that would comply the reliability requirement $R(t) = 0.99999$. The solution is to use the equation (11) for unknown nominal cross-section μ_A. First, tension of the rod should be determined with the equation $N = Q/A$ [N/cm^2] if the rod cross-section is defined in cm^2. The randomly variable tension of the rod whose value is Y shall have the mean value $\mu_Y = \frac{\mu_Q}{\mu_A} = \frac{12.7 \cdot 10^8}{\mu_A}$ [Pa] and the mean-root-square error $\frac{(\mu_Q^2, \sigma_A^2 + \mu_A^2 \sigma_Q^2)}{\mu_A^4} \rightarrow \sigma_Y^2 = \frac{1.91 \cdot 10^8}{\mu_A}$ [Pa]. The tension in the rod follows approximately normal distribution $N(\frac{12.7}{\mu_A}, \frac{1.91}{\mu_A}) \cdot 10^8$ [Pa]. The standard normal distribution function tables [3] show $t = 4.265$ at $R(t) = 0.99999$. Substitution in the equation (13) results in $4.265 = \frac{3.5 - 12.7/\mu_A}{\sqrt{(0.35)^2 + (\frac{1.91}{\mu_A})^2}}$. When this equation is solved for μ_A the required minimum cross-section $\mu_{A\,min} = 7.63$ cm^2 and its mean-root-square error $\sigma_A = 0.05\,\mu_A = 0.3815$ cm^2.

4 Conclusion

Reliability designing with variables actually represented by statistic models that us construction failure-proof operation probability R rather than the conventional safety factor offers tools to solve numerous constructional key problems. First of all, it is systematic analysis of reliability for the questioned constructional element and last but not least the reliability designs including the theoretical reliability requirements [10]. There is a very close relation between this and optimum construction as the determination of optimum dimensions may enhance with the determination of optimum production and material costs. A simple example showed the procedures of reliability designing for static load with normal distribution of random variables. It should be noted that the basic procedures remain the same also for construction design when load is dynamic in character and the random variables take more complex forms of distribution. Of course, the equations for calculation are more complex then. The world leading automobile industry companies have proved the advantage of reliability design in case of large scale production as the higher cost of reliability design pay shortly back in saved material, energy, labour and also in the increased reliability rate of the final product. Other advantages of this method include efficient planning of spare parts, maintenance and more.

Acknowledgment

Presented work has been prepared with the support of the Ministry of Defence of the Czech Republic, Partial Project for Institutional Development and Specific Research, Department of Combat and Special Vehicles, University of Defence, Brno.

References

1. F. Bohacek, *Parts and Mechanisms of Machines I. Princiles of Design*. University of Technology Brno, (1981)
2. P. Klimes, *Machine Parts and Mechanisms I. Reliability, sizing, joints and shafts*. Academic publishing house CERM Ltd., Brno, (2003)
3. P. D. T. O΄Connor, D. Newton, R. BROMLEY, *Practical Reliability Engineering*. John Wiley & Sons, LTD (Fourth Edition), ISBN 978-0-470-84462-5 (2002)
4. V. K. Way, R. Prasad, A. Frank, T. Ching, L. Hwang, *Optimal Reliability Design*. Cambridge University Press. ISBN 0-52-1031-915 (2006)
5. Institute of Electrical and Electronics Engineers IEEE Standard Computer Dictionary: *A Compilation of IEEE Standard Computer Glossaries*. New York, NY ISBN 1-55937-079-3 (1990)
6. J. Sedlacek, *Theory of Reliability of Complex Mechanical Systems*. CTU Publishing Center, Prague, (1982)
7. J. T. Yang, *An Outline of Scientific Writing*. World Scientific Publishing, London, (1995)
8. RCM II, Reliability Centered Maintenance, Second edition, page 250-260, the role of Actuarial analysis in Reliability (2008)
9. Hoang Pham (editor). *Handbook of Reliability Engineering*. Springer, New Jersey. p 696, (2003)
10. J. Stodola, *The basic of Reliability Design*. Lerning text. University of Defence in Brno, (2017)
11. J. Stodola, *Operational Reliability of Automotive I: Theoretical part. Lerning text*. Military academy in Brno, (1984)
12. J. H. Saleh, K. Marais, *Highlights from the Early History of Reliability Engineering*. Reliability Engineering and System Safety, Volume 91, Issue 2, Pages 249–256 (2006)
13. D. J. Smith, *Reliability Maintainability and Risk Practical Methods for Engineers Including Reliability Centred Maintenance and Safety* (2011)
14. J. Janko, *Statistical Tables*. Publishing house of the Czechoslovak Academy of Sciences, Prague, (1958)
15. Z. Karpisek, *Matematics: Statistics and Probability*. Academic publishing house CERM Ltd. Brno, (2003)
16. JFederal Aviation Administration *System Safety Handbook* (PDF). U.S. Department of Transportation. Retrieved 2 June 2013
17. MIL-HDBK-338B Electronic Reliability Design Handbook, U.S. Department of Defense, New York, (1998)
18. S. Distefano, A. Puliafito: *Dependability Evaluation with Dynamic Reliability Block Diagrams and Dynamic Fault Trees.* IEEE Trans. Dependable Sec. Comput. 6(1): 4–17 (2009)
19. R. Denney, *Succeeding with Use Cases: Working Smart to Deliver Quality*. Addison-Wesley Professional Publishing, (2005)