ENGINEERING DESIGN FROM A SAFETY PERSPECTIVE

Cristian Iorga, Alain Desrochers, and Cécile Smeesters
Department of Mechanical Engineering, Faculty of Engineering, Université de Sherbrooke
Cristian.Iorga@USherbrooke.ca, Alain.Desrochers@USherbrooke.ca, and Cecile.Smeesters@USherbrooke.ca

Abstract – *Engineering design is an iterative decision-making process involving interactions between three elements: geometry, materials and loads. The objective is to provide an optimum combination of these design parameters. Unfortunately, the absolute optimum can rarely be achieved because the design criteria typically place counter opposing demands and uncertainties must be accommodated.*

To this end, the integration of both deterministic and stochastic methods into the product development process is encouraged. The deterministic method allows designers to calculate a design safety factor based on the uncertainties of a loss-of-function parameter and a maximum allowable parameter. Stochastic methods are based on the statistical nature of the design parameters and focus on the reliability of the design.

Links between these elements will thus be emphasized and supported with examples from the recreational product industry.

Keywords: Engineering Design, Reliability, Design Safety Factor, Design Parameters.

1. INTRODUCTION

A key strategy in the PDP *(Product Development Process)* is to avert failure of a machine or structure by predicting and analyzing potential failure scenarios at the design stage, before the machine is built [1, 9, and 11]. By identifying the loads, the governing failure modes and tentatively selecting the appropriate candidate material, the failure prediction scenarios provide a basis for choosing the optimal combination of design parameters: geometry, material and loads. Ideally, if load cases and material characteristics were perfectly known, the geometry of machine parts could readily be determined by simply making sure that operating loads or stresses never exceed the strengths at the most critical zones of the part [9].

The topics outlined in this paper will introduce students to product related issues such as safety and reliability. The examples that follow each topic also provide students with a better understanding of the design from a failure prevention perspective.

2. DETERMINISTIC APPROACH TO FAILURE PREVENTION

Early in the PDP, the geometry of a part is usually determined by first defining a *design-allowable value* for whatever *loading parameter* is selected, whether it is deflection, stress, strain, load, speed, etc. [2]. For example, to determine the design-allowable force *(P_d)*, the *critical failure level* corresponding to the selected loading parameter *(L_{fm})* is divided by a *design safety factor (n_d)* to account for variabilities and uncertainties identified up-stream in the design process. Thus, following the calculations the maximum operating value of the selected loading parameter can be determined and it is less than the design-allowable value [1, 2, 9, and 11]. Mathematically, this may be expressed as:

$$P_d = \frac{L_{fm}}{n_d} \quad \text{(a)}$$

The selected loading parameter is often the stress and the critical failure level will be the *material strength corresponding to the governing failure mode* [1, 5, and 6]. Hence, from an engineering point of view, a more usual form of (a) is:

$$\sigma_d = \frac{S_{fm}}{n_d} \quad \text{(b)}$$

Where σ_d is the design-allowable stress, S_{fm} is the strength of the material corresponding to the governing failure mode, and n_d is the design safety factor. To provide a safe design, the engineers have to calculate the dimensions so that the maximum operating stress levels are equal to or less than the design-allowable stress (σ_d) [1, 9, and 11].

The deterministic method, suggested by Jack A. Collins [11], uses a series of semi-quantitative smaller decisions that may be weighted and empirically recombined to calculate an acceptable value for the design safety factor, tailored to any given specific application [9, 11]. Even experienced designers find this approach valuable when faced with designing a new product or

improving an existing one. For an appropriate selection of a design safety factor, this method considers separately each of the following eight *rating factors* [11]:

1. The precision with which the forces, deflections, or other failure-inducing factors can be determined;
2. The precision with which the stresses or other loading parameters can be determined from the forces or other failure-inducing factors;
3. The precision with which the strengths or other measures of failure can be determined for the selected material in the appropriate failure mode;
4. The need to reduce weight, space, money;
5. The seriousness of the consequences of failure in terms of human life and/or property damage;
6. The quality of manufacturing;
7. The conditions of operation *(corrosion, temperature, off-road, etc.)*;
8. The quality of inspection and maintenance possible during the product life.

A semi-quantitative estimation could be made by assigning to each rating factor a *rating number*, ranging in value from -4 to +4 [11]. A Likert scale was used to provide values to these rating numbers (*RNs*) and they have the following meanings:

- *RN=0* (*No need* to modify n_d);
- *RN=1* (*Mild need* to modify n_d);
- *RN=2* (*Moderate need* to modify n_d);
- *RN=3* (*Strong need* to modify n_d);
- *RN=4* (*Extreme need* to modify n_d).

Moreover, if the safety factor needs to be increased, the selected rating number is assigned a positive (+) sign. If the safety factor needs to be reduced, the selected rating number is assigned a negative (-) sign [1, 11].

The next step is to calculate the algebraic sum, *t*, of the eight rating numbers, giving:

$$t = \sum_{i=1}^{8} RN_i \quad \text{(c)}$$

Using the results from (c), the design safety factor, n_d, may be empirically estimated from:

$$n_d = \begin{cases} 1 + \dfrac{(10+t)^2}{100} & \text{for } t \geq -6 \quad \text{(d)} \\ 1.15 & \text{for } t < -6 \quad \text{(e)} \end{cases}$$

Using this method, the design safety factor will never be less than 1.15, and will rarely be larger than 4 or 5. This range is broadly compatible with the usual list of suggested safety factors found in most design books [7, 9, and 11].

However, special caution must be taken in setting the design safety factor (n_d) [1]:

- Avoid "chained" safety factors, i.e. applying safety factors on several elements in the same computation (ex.: doubling both the maximum load and the member section in a stress calculation, leading to a $n_d = 2 \times 2 = 4$);
- Avoid hidden safety factors such as those arising from the systematic rounding up of numbers in design parameter calculation sequences, to be on the conservative (safe) side;
- Consider adapting safety factors to reflect the specific risk of the various systems in a product (ex.: structural vs. aesthetic parts);
- Choose appropriate safety factors on serial mechanical components to establish a "fuse" (ex.: $n_d(key) < n_d(shaft)$);
- Verify whether the global safety factor of any given product remains acceptable. The global safety factor will be the lowest safety factor of all subsystems (weakest link);
- Verify that there is no standard, guiding the values of the safety factor for some specific products critical to user safety (ex.: boiler or elevator).

Moreover, several considerations regarding safety factors have been identified:

- Safety factors are an engineering expression of the customer or product requirements from a resistance standpoint;
- Safety factors can be seen as an insurance against design risks;
- Safety factors can embed the expertise gained using a stochastic approach or other approaches based on experimental testing;
- Safety factors are generally kept confidential by companies;
- If disclosed, safety factors could be misused in trials, hence leading to liability in case of accident;
- Safety factors must nevertheless be internally documented for product traceability.

Example 1

The method outlined in this section is applied to calculate the safety factor for the frame of a new recreational product. In this instance, the engineers have been asked to calculate the appropriate safety factor for a new structure.

The project may be regarded as "average" in many respects, and the material properties are very well known. Moreover, the need to conserve weight and money is

strong, there is also a genuine concern about threat to life and property if the part fails, and the quality of inspection and maintenance is regarded as "satisfactory".

In this context, the engineer's task is to determine the appropriate safety factor for this part.

Solution 1

Based on the given information, the rating numbers assigned to each of the eight rating factors might be chosen as follows:

1. Accuracy of applied loads = 0;
2. Accuracy of stress calculation = 1;
3. Accuracy of material stress = -1;
4. Need to conserve weight and money = -3;
5. Seriousness of failure on life and properties = +3;
6. Quality of manufacturing = 0;
7. Conditions of operation = 0;
8. Quality of inspection and maintenance = +1.

The next step is to calculate the algebraic sum (*t*), of the eight rating numbers:

$$t = 0 + 1 - 1 - 3 + 3 + 0 + 0 + 1 = 1$$

Since $t \geq -6$, the recommended value for an appropriate design safety factor for this application would therefore be:

$$n_d = 1 + \frac{(10+1)^2}{100} = 2.21$$

This approach represents a rough estimation of the safety factor that would be made in the earlier steps of product design. The available statistical data concerning the eight rating factors will enable the optimization of the design. The next section will thus emphasize the need for stochastic approaches to optimize and validate the design criteria.

3. STOCHASTIC APPROACH TO FAILURE PREVENTION

In order to obtain quantitative estimates of the percentage of anticipated failures, we must look into the nature of the distribution curves for significant stress and strength [3, 7 and 12].

By definition, reliability (*R*) is the probability that the strength exceeds the stress, or:

$$R = P\{S_{fm} > \sigma_d\} = P\{S_{fm} - \sigma_d > 0\} \quad \text{(f)}$$

The normal distribution is the probability density function most commonly used by designers for the calculation of product reliability [3, 10 and 11]. The probability density function *f(x)* for the normal distribution can be expressed as follows:

$$f(x) = \frac{1}{\hat{\sigma}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\hat{\mu}}{\hat{\sigma}}\right)^2} \quad \text{for } -\infty < x < \infty \quad \text{(g)}$$

where *x* is a random variable such as stress or strength, $\hat{\mu}$ is the estimated *sample mean*, and $\hat{\sigma}$ is the estimated *sample standard deviation*, where:

$$\hat{\mu} = \frac{1}{N}\sum_{i=1}^{N} x_i \quad \text{(h)}$$

$$\hat{\sigma} = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \hat{\mu})^2} \quad \text{(i)}$$

In the expressions (h) and (i), N is the number of parts that are integrated in reliability analyze. Another measure of dispersion is the *variance* ($\hat{\sigma}^2$), which is equal to the square of the standard deviation.

''*Both variance and standard deviation are measures of dispersion,*, [1].

The conventional expression of a normal distribution is:

$$x \overset{d}{\Rightarrow} N(\hat{\mu}, \hat{\sigma}) \quad \text{(j)}$$

The expression (j) is to be read as "*x* is distributed normally with mean $\hat{\mu}$ and standard deviation $\hat{\sigma}$" [11].

The corresponding normal cumulative distribution function, *F(X)*, can be expressed as follows:

$$F(X) = P\{X \leq X_0\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{X_0} e^{-t^2/2} dt \quad \text{(k)}$$

$$X = \frac{x - \hat{\mu}}{\hat{\sigma}} \quad \text{(l)}$$

where *X* represents the standard normal variable, normally distributed with a mean of 0 and a standard deviation of 1. X_0 is any specified value of the random variable *X* [1, 4, 9, 11 and 12]. Thus, the *normal distributions* with mean $\hat{\mu}$ and standard deviation $\hat{\sigma}$ can be transformed into a *standard normal distribution* using equation (l) [3].

The normal distributions can be defined by $\hat{\mu}$ and $\hat{\sigma}$. Hence, they are also called *two-parameter distributions*. When several normally distributed random variables are summed, the result is also normally distributed with a mean equal to the sum of each distribution means and a

standard deviation equal to the square root of the sum of each variance [11].

Therefore, when $f(\sigma_d) = f(\sigma)$ and $f(S_{fm}) = f(S)$ are both normal probability density functions, the random variable $y = (S_{fm} - \sigma_d) = (S - \sigma)$ used in equation (f) is also normally distributed with a mean and standard deviation of:

$$\hat{\mu}_y = \hat{\mu}_S - \hat{\mu}_\sigma \quad \text{(m)}$$

$$\hat{\sigma}_y = \sqrt{\hat{\sigma}_S{}^2 - \hat{\sigma}_\sigma{}^2} \quad \text{(n)}$$

Finally, the reliability *R* may be expressed as:

$$R = P\{S_{fm} - \sigma_d > 0\}$$

$$= P\{y > 0\}$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\frac{\hat{\mu}_y}{\hat{\sigma}_y}}^{\infty} e^{-t^2/2} dt$$

$$= \frac{1}{\sqrt{2\pi}} \int_{-\frac{\hat{\mu}_S - \hat{\mu}_\sigma}{\sqrt{\hat{\sigma}_S{}^2 - \hat{\sigma}_\sigma{}^2}}}^{\infty} e^{-t^2/2} dt \quad \text{(o)}$$

$$Y = \frac{y - \hat{\mu}_y}{\hat{\sigma}_y} \quad \text{(p)}$$

where Y is the standard normal variable.

Example 2

It is assumed that for the structural application presented in example 1 a tubular section of $D = 26\text{mm}$ (outside diameter) and $d = 20\text{mm}$ (inside diameter) made of 2024-T4 aluminum had been chosen.

Experimental data for the material tested under conditions that closely match those of the actual operating conditions indicate that the fatigue strength is normally distributed with a mean value of 220MPa and a standard deviation of 30MPa. The cyclic load on the tube has a nominal value of 22kN, but this load has been found to actually be a normally distributed random variable with a standard deviation of 1kN.

The reliability goal for this part was established as $R = 99.5\%$.

With these data, the engineers have to: a) verify the safety factor established up-stream for this design process; b) find the actual reliability of the tube and optimize its geometry until the reliability goal is met.

Solution 2

a) First, the nominal design stress is:

$$\sigma_d = \frac{P}{A}$$

$$= \frac{P}{\frac{\pi}{4}(D^2 - d^2)}$$

$$= \frac{4(22\text{kN})}{\pi((26\text{mm})^2 - (20\text{mm})^2)}$$

$$= 101.5\text{MPa}$$

Based on fatigue criteria, the safety factor is thus:

$$n_d = \frac{S_{fm}}{\sigma_d} = \frac{220\text{MPa}}{101.5\text{MPa}} = 2.17 \cong 2.21$$

Hence, the initial safety factor is verified.

b) From the data provided $P \overset{d}{\Rightarrow} N(22\text{kN}, 1\text{kN})$, $S_{fm} \overset{d}{\Rightarrow} N(220\text{MPa}, 30\text{MPa})$, the calculated mean stress is $\hat{\mu}_\sigma = 101.5\text{MPa}$ and the estimated standard deviation is:

$$\hat{\sigma}_\sigma = \frac{\hat{\sigma}_P}{\frac{\pi}{4}(D^2 - d^2)}$$

$$= \frac{4(1\text{kN})}{\pi((26\text{mm})^2 - (20\text{mm})^2)}$$

$$= 4.6\text{MPa}$$

Hence

$$\sigma_d \overset{d}{\Rightarrow} N(101.5\text{MPa}, 4.6\text{MPa})$$

The lower limit of the reliability integral in (o) may thus be calculated as:

$$Y_0 = -\frac{\hat{\mu}_S - \hat{\mu}_\sigma}{\sqrt{\hat{\sigma}_S{}^2 - \hat{\sigma}_\sigma{}^2}} = -\frac{220\text{MPa} - 101.5\text{MPa}}{\sqrt{30\text{MPa}^2 - 4.6\text{MPa}^2}} = -4.00$$

From tables of the cumulative distribution function for the standard normal distribution, the reliability corresponding to $Y = -4$ may be read as:

$$R(-y) = 1 - R(y) = 1 - P\{y > 0\} = 0.99997$$

It has to be emphasized here that no strength-influencing factors such as surface finish, corrosion, and

so forth, have been considered in this example. A more accurate prediction could be made by considering such factors.

Table 1 presents the results of several iterations that have been made to achieve the initial objective for the application: *A reliability of 99.5%*.

Table 1: Dimensional optimization of tubing size.

Iteration	Geometry	n_d	*Y*	*R*
0	*D*26-*d*20	2.17	-4.00	99.9%
1	*D*25-*d*20	1.77	-3.24	99.9%
2	*D*24-*d*18	1.98	-3.68	99.9%
3	*D*22-*d*16	1.79	-3.30	99.9%
4	*D*23-*d*18	1.61	-2.84	99.8%
5	*D*22-*d*18	1.26	-1.55	94.0%
6	*D*23-*d*18.5	1.46	-2.40	99.2%
7	***D*23-*d*18.3**	**1.52**	**-2.59**	**99.5%**

Owing to the use of available statistical data, the stochastic approach provides more precision in making design decisions about materials and dimensions, and at the same time, preserves the designer's ability to account for design uncertainties and variability. In this example, it could be seen that the reliability of the part was initially too high compared to reliability goal of the project. Consequently the approach entailed backward iterations to search for other, more appropriate, combinations of geometry and loads.

4. OPTIMIZATION OF THE SAFETY FACTOR AS A RESULT OF HIGHER RELIABILITY DATA

Rather than choosing between the two approaches, a more productive viewpoint might be to combine the best attributes of each for making clever design decisions. Thus, where well-defined probabilistic data are available for describing strength, loading and manufacturing practices, this quantitative statistical information might be integrated piecewise in the design safety factor approach. As more precise probabilistic data are incorporated, the rating numbers *(RNs)* tend to be driven toward more negative values, since more precise information would result in a drive to lower the design safety factor.

Errors in the deterministic approach (safety factors) can be detected by the stochastic approach (reliability) and vice-versa.

The integration and the application of both deterministic and stochastic approaches into undergraduate projects represent an original method from an educational stand point. Integrating these approaches into the product development process represents an original way to provide the students with more precise data, helping them make more sensible decisions concerning design parameters (materials, geometry and loads) while preserving the student's aptitude to take into account the uncertainties that are not supported by statistical data.

The proposed approaches also allow the students to perform design iterations throughout the steps of the product development process and to optimize their initial concept depending on the new data collected during this process. This method also has a significant influence on the robustness of the final product by preventing both over-design and poor-design, hence increasing the design team's competencies and helping the students to look back at the product requirements and client needs with the aim of providing the optimum solution for each design problem encountered.

5. CONCLUSIONS

The article presents two methods of failure prevention by calculating a reasonable design safety factor and by estimating an appropriate reliability goal for a structural part. The product optimization was also integrated into the design process, by performing stochastic analyzes and finally choosing the optimal combination of design parameters with the correspondingly appropriate safety factor for this part.

Using the statistically significant new strength data in example 2 results in a design safety factor reduction of about 30% *(from the initial safety factor of 2.17 to the optimized safety factor of 1.52)*. It should however be cautioned that the 30% reduction in design safety factor does not necessarily correspond to 30% increasing of the design-allowable stress. The reason for this is that the limit value of the governing failure mode used in the calculation of the design-allowable stress depends upon the choice of an appropriate reliability objective for the structure.

Although most real design situations involve fluctuating loads that produce multi-axial states of cyclic stress, no consensus has yet been established on the best approach for the prediction of failure under such conditions of stress. However, the approach adopted by researchers involves the concept of an equivalent stress to define a uni-axial equivalent to the real multi-axial state of cyclic stresses, including both the alternating stress amplitudes and mean stresses. More information and details concerning this approach is provided in the references [1, 9, and 11].

The following conclusions can be made based on the proposed methods outlined in this paper:

1. Selection of a safety factor must be undertaken with care to avoid the negative consequences associated with the selected values *(safety factor too small = high probability of failure; safety factor too large = cost, weight or size too high)*;

2. Assessing a realistic reliability goal requires a good knowledge of the limitations in the simulation

   programs used, the mechanical properties of the material chosen and the operational details of the product (load cases);
3. Both, the deterministic and stochastic methods to prevent failure have a very significant influence on the optimization of several design criteria (ex.: cost, weight and manufacturing processes);
4. The approaches outlined in this paper will be applied to undergraduate projects and integrated in the mechanical engineering curricula at the Université de Sherbrooke.
5. The deterministic approach will allow students to estimate a reasonable safety factor while the stochastic approach will provide a more realistic goal for their design.

If we were to make a review of the fundamental steps of the product development process detailed by Iorga and Desrochers [8], the deterministic method would be performed at the design criteria analysis phase (more specifically, 1st rank quantitative criteria). Conversely, the stochastic method would be performed either at the loads identification step (preliminary design) or after the laboratory and physical tests (detailed design), depending on the availability of pertinent data.

The approaches outlined in this paper will help students involved in undergraduate projects to make sound engineering decisions regarding the safety and reliability of their product and to understand the place of these approaches in the product development process.

References

1. Budynas-Nisbet (2008), *Shigley's Mechanical Engineering Design (8th edition)*, McGraw-Hill's, 1054 pp. {ISBN 0-390-76487-6}
2. Burdekin F. M., (2007), *General principles of the use of safety factors in design and assessment*, Engineering Failure Analysis, pp. 420-430.
3. Castillo E, Losada MA, Mı´nguez R, Castillo C, Baquerizo A., (2003), *An optimal engineering design method that combines safety factors and failure probabilities. Application to rubble mound breakwaters*. J Waterways, Ports, Coastal Ocean Engng, ASCE 2003.
4. Cheol-Eung Lee, Seung-Woo Kim, Dong-Heon Park, Kyung-Duck Suh, (2011), *Target reliability of caisson sliding of vertical breakwater based on safety factors*, Coastal Engineering pp. 167-173.
5. Ching J., Hsieh Y., (2009), Updating real-time reliability of instrumented systems with stochastic simulation, Probabilistic Engineering Mechanics, pp. 242-250.
6. Clausen J., Hansson S., Nilsson F. (2006), *Generalizing the safety factor approach*, Reliability Engineering and System Safety, pp. 964-973.
7. Freudenthal AN. *Safety and the probability of structural failure*. Trans ASCE 1956; 121:1337–97.
8. Iorga C., Desrochers A., (2011), *Product Modeling, Evaluation and Validation at the Detailed Design Stage*, CEEA 2011(Canadian Engineering Education Association), (St. John's NL. 6-8 june 2011), 4 pp., 2011.
9. Marshek K. and Juvinall R. (2006), *Fundamentals of Machine Component Design (4th edition)*, New Jersey: John Wiley & Sons, 899 pp. {ISBN 978-1118-01289-5}
10. Pradlwarter H. J., Schuëller G. I., Koutsourelakis P.S., Charmpis D. C., (2007), *Application of line sampling simulation method to reliability benchmark problems*, Structural Safety pp. 208-221.
11. Staab G., Busby H. and Collins J. A. (2010), *Mechanical Design of Machine Elements and Machines (2nd edition)*, New Jersey: John Wiley & Sons, 890 pp. {ISBN 978-0-470-41303-6}
12. Vidosic, Joseph P. (1957), *Machine Design Projects*, Ronald Press, NY.