PROCEEDINGS OF ICOSSAR'93 – THE 6TH INTERNATIONAL CONFERENCE ON STRUCTURAL SAFETY AND RELIABILITY / INNSBRUCK / AUSTRIA / 9-13 AUGUST 1993

Structural Safety & Reliability

Edited by

G.I. SCHUËLLER
University of Innsbruck, Austria
M. SHINOZUKA
Princeton University, New Jersey, USA
J.T.P. YAO
Texas A & M University, College Station, Texas, USA

OFFPRINT

A.A. BALKEMA / ROTTERDAM / BROOKFIELD / 1994

Structural Safety & Reliability, Schuëller, Shinozuka & Yao (eds) © 1994 Balkema, Rotterdam, ISBN 90 5410 357 4

Quality assurance in structural design

S. Engelund & R. Rackwitz
Technical University of Munich, Germany

ABSTRACT The fact that a large number of structural failures is caused by human errors committed during the design emphasizes the necessity of an efficient and documented quality assurance system. This paper is concerned with checks of the design, only. General models which can be used to determine the occurrence and detection probabilities of human errors are proposed. On this basis various known quality assurance systems implemented in different countries and for different projects are compared with respect to efficiency optimal total cost and operational failure probabilities.

1. INTRODUCTION

Due to the increasing demands for high "quality" of structural engineering and the fact, that a large number of structural failures are caused by human errors committed during the design (see e.g. Matousek and Schneider [3]), much effort is made to develop and to execute schemes for the assurance of "quality" of structural design. A number of different schemes for the quality assurance of engineering structures are implemented in different countries and for projects of different type.

Given a complete description of the purpose, performance and requirements, the design process can be modeled by three phases: Concept, Design and Check (see figure 1)

Figure 1: The design process.

In the concept phase all necessary decisions and assumptions, which form the basis of the specific design task, are made. In the second phase the actual design involving the calculations and the appropriate detailing together with the necessary documentation is performed by a person or a group of persons, who also perform self-checking to a certain degree. In the third phase the results obtained in the first and second phase are checked by a person of group of persons. The various activities in the three phases can be performed by the same person or group of persons or different ones. They necessarily are performed sequentially but there are feed backs to earlier phases. The way in which the phases and their interactions are organized together with the assignment of persons or groups of persons to various activities, the specification of the professional qualifications and the distribution of responsibilities defines a quality assurance system. Any such system of course requires a suitable agreement about financial organization, payments, reimbursements etc. Obviously a variety of quality assurance systems is possible and are effectively in use

2. CHECKING SCHEMES

It is not suitable to discuss all checking schemes presently in use. The following three systems are considered as typical and might cover by and large the majority of systems.

SCHEME 1: In this system all tasks are performed by the same engineer. Usually certain qualifications are required depending on the type and complexity of the structure to be designed. The advantage of this system is that the engineer does not have to use time in order to understand the problem. The efficiency of checking, therefore, is high throughout the whole checking process. However, the basic assumptions and decisions are only seldom questioned once they are made.

SCHEME 2: No special qualifications are demanded of the engineer who performs the initial design and the calculations, but the check has to be made by and independent and experienced engineer. This engineer usually has to fulfill some pre specified qualification requirements. In this case the checker will use some time in the beginning of the check as he is trying to understand the problem. Because of the independence, it is expected that the errors in the initial assumptions and decisions are detected.

SCHEME 3: In this system the checking is performed by a person or group of persons within the same company, where the design was performed. The checking group, however, is organizationally independent from the design group. In this case there is often a kind of negative correlation between the designer and checker, so that when the designer is inexperienced the checker is experienced and vice versa. As by the second system the checker will need some time to understand the problem before the check becomes efficient. By this system, however, the designer and checker are likely to share the same experience and tradition of doing things. This reduces the probability, that the checker detects the errors in the assumptions and decisions.

3. VALUATION CRITERIA

A judgment and ranking of the three methods can be made on various grounds but a fair judgement appears possibly only by comparing the optimal expected cost to society, $E[C_T]$ for a given structural element, which has been dimensioned according to a specific set of rules.

$$E[C_T] = C_D(t_D;A_D) + C_{QA}(t_{QA};A_C) + C_C + P_f(t_D;A_D;t_{QA};A_C)C_F \qquad (1)$$

where $C_D(t_D;A_D)$ are the costs of the design as a function of the time spent on the design, t_D and the qualification of the designer A_D, $C_{QA}(t_{QA};A_C)$ are the cost of quality assurance as a function of the time spent on quality assurance, t_{QA} and the qualifications of the checker, A_C. C_C is the cost of construction, C_F is the cost of failure and P_f is the probability of failure. The cost of design of quality assurance are proportional to the time spent on the tasks

4. HUMAN ERROR

Human error can be defined as violations of the design rules, which will change the reliability, serviceability or economy of the structure. A more exact and widely accepted definition of human error is, that it is a noncompliance with code, or more generally, a significant deviation from acceptable practice. This definition excludes unforeseen events, "acts of god", and it is in compliance with legal practice. It further excludes gross negligence and criminal actions. But it does not account for errors in the accepted practice, and it leaves the problem of defining, what is acceptable practice.

The load on a structural element, *S*, will by assumption not be affected by human errors. The coefficient of variation of the resistance, *R*, is a constant, which depends on the quality control of the material. The purpose of the design process is to determine the mean value of the resistance *R*, so that the probability of failure becomes "small". The effect of the human errors can, therefore, be introduced by the variable ε, which describes the change of the mean value of the resistance.

$$\Psi_R = \mu_R \varepsilon \qquad (2)$$

μ_R is the mean value of the resistance in case no errors have occurred, and ε describes the effect of the errors in the design. ε is a function of the number of errors and the magnitude of each of these errors. The magnitude of an error, *e*, is defined as

$$e = \frac{\mu_R^e}{\mu_R} \qquad (3)$$

where μ_R^e is the mean value of the resistance with the error included and μ_R the mean value of the resistance of the error-free structure.

It is convenient to introduce two classes of errors: concept and design errors. The concept and design errors are errors, which are made in the concept and design phase of the design process, respectively. The following limited number of concept errors, which are assumed to be the most important are included in the model.

- An error in the geometry of the structure
- An error in the boundary conditions
- An error in loads or load cases
- An error in the selection of the relevant failure mode
- An error in the selection of the structural analysis model

It is evident, that all the tasks in the concept phase will either be performed correctly or wrongly. Each of these types of errors occur only once. For the analysis of a design task it is in most cases sufficient to include the following types of design errors

- Error in calculator calculations
- Error in table look-up
- Error in ranking

The calculations are performed in a number of steps, each of which correspond to a mathematical operation (multiplication, addition, ...). The probability of making an error in each of these steps is assumed to be roughly the same and all errors are assumed to be independent. Then the probability that j errors remain in the design can then be modeled by a Poisson process

$$P_E(j) = \frac{(\lambda p_E)^j}{j!}\exp(-\lambda p_E) \qquad (4)$$

where λ is the intensity, which depends on the complexity of the design task and p_E is the probability that a calculation error remains. This model has also been suggested by Nessim [5]. The logarithm of the magnitude of the error is normally distributed with mean 0 and standard deviation 2.03 (Melchers and Harrington [4]). The decision about which table look-up errors and errors by ranking to include in the analysis, has to be based on information about the occurrence probability and the effect of each of the potential errors.

5. CHECKING MODEL

The checking consists of two parts: a self checking taking place during the design process and a detailed checking after the design. For self checking the model suggested by Stewart and Melchers [7] is used. For detailed checking it is assumed that its success depends on the complexity of the design task, the magnitude of the error, the qualification of the checker and the time spent in checking. Let $q_E(e,t)de$ be the probability of an error in the (small) interval *de*, when the time spent checking is *t*.

$$q_E(e,t) = f_{E_o}(e)\,P(\text{nondetection of } E \text{ at } t = t \mid E = e \text{ at } t = 0) \qquad (5)$$

where f_{E_o} is the density of the error before checking. It should be noted that by assumption the error is certain to occur. The density function of the error after the time t spent checking is

$$f_E(e,t) = \frac{q_E(e,t)}{\int q_E(e,t)de} \qquad (6)$$

In the following the notation will be used

$$P(\text{nondetection of } E \text{ at } t = t \mid E = e \text{ at } t = 0) = Q(e,t) \qquad (7)$$

Following Lind´s model [1] the rate of decrease of this function is proportional to the probability that the error has not yet been detected, $Q(e,t)$, and proportional to a function *h* of the magnitude of the error. According to Stewart and Melchers (7) the efficiency of the check is not constant, and therefore a function $g(t)$ is introduced. $g(t)$ describes the efficiency of the check as a function of the complexity of the problem and the qualifications of the checker. The decrement of the non detection probability is also assumed to be proportional to $g(t)$. This leads to the following equation:

$$\frac{\partial Q(e,t)}{\partial e} = -h(e)g(t)Q(e,t) \quad \Leftrightarrow$$
$$Q(e,t) = c\exp\left[-h(e)\int_0^t g(\tau)d\tau\right] \qquad (8)$$

where $c = 1$ because $Q(e,t) = 1$ for all *e* at $t = 0$.

5.1 *Concept errors*

The concept errors are discovered in the initial phase of the check. where the checker is trying to understand and reevaluate the design problem. It is assumed that if the checker does not detect the error in the initial phase the error will never be discovered. The efficiency with respect to concept errors is zero at $t = 0$. It increases rapidly during the first part of the check, reaches a maximum and then decreases to zero. The probability that a concept error is detected does not depend on the magnitude of the error. The function $h(e)$ is constant. The constant can be chosen as unity. This implies that the distribution of the error does not depend on the time spent in checking. If furthermore the duration of the check exceeds the initial phase where the check for concept errors is made then, the probability that an error remains in the design is constant. Therefore, it is only necessary to know the probability that the error is detected.

SCHEME 1: When the check is performed by the designer, it is assumed that the probability, of detecting a concept error is zero

SCHEME 2: In case the check is performed by an independent checker, the probability that errors in the geometry and boundary conditions are detected is assumed to be one. There exists a large number of such errors and it is unlikely that an independent checker makes the same error. The probability that the independent checker does not detect errors in the load cases and method is assumed to be equal to the probability that the checker would have made these errors.

SCHEME 3: As by scheme 2 it is assumed that errors in the geometry and boundary conditions are certain to be detected. If the designer and the checker works in the same firm, have been educated at the same university or in some way share the same tradition for selecting load cases and analysis method, the probability that such errors remain is likely to be larger than if no dependence exists.

5.2 *Design errors*

The probability that a design error is detected depends on the magnitude of the error. It is further assumed that if infinite time is spent in checking the design errors are certain to be detected. This implies that the check for design errors cannot simply be modeled by a detection probability for each error. It is assumed that large errors are easier detected than smaller errors, and that the value of $h(e)$ is the same for errors which result in a decrease as well as for errors which increase μ_R by a given factor. The last assumption is not fully correct because errors which reduce the reliability of the structure are probably detected with larger probability than errors which increase the reliability. The assumption therefore leads to a conservative estimate of the failure probability.

As the error magnitude e is defined as the change of the mean value of the resistance of the structure, then $e = 1$ implies $h(e) = 0$. Stewart and Melchers [7] state that $h(e)$ only varies little with e. The simplest possibly model is

$$h(e) = |\ln(e)|^{\alpha} \tag{9}$$

This model is valid for all three schemes of checking, and α does not depend on the scheme.

The function $g(t)$ describes the efficiency of the check as a function of the time spent checking. It is evident, that the efficiency depends on the checking method.

SCHEME 1: When the check is performed by the designer the checking efficiency is assumed to be constant

$$g(t) = a \tag{10}$$

where a depends of the complexity of the problem and the qualification of the checker.

SCHEME 2: The efficiency will be small in the beginning as the checker is making an attempt to understand the problem. Thereafter, $g(t)$ increases to reach a constant value. It is assumed that the increase in the efficiency will be very small in the beginning, which means that the derivative of $g(t)$ at $t = 0$ is small. It is evident that the function depends on the complexity of the problem and the qualification of the checker. If the qualification of the checker is bad or the problem very complex it can reasonable be assumed that $g(t)$ will reach the constant at a later time. Also its final value might be smaller than for simple problems or better qualifications. A simple function which can describe the efficiency of the check is:

$$g(\tau) = a(1-(a\tau+1)\exp[-a\tau]) \tag{11}$$

where a for the same level of qualification takes on roughly the same value as by scheme 1.

SCHEME 3: The checking efficiency for method 3 is equal to the checking efficiency for scheme 2. The fact that the checker and designer might share the same knowledge and are prone to make the same concept errors does not effect the checking efficiency with respect to design errors.

6. CALCULATION OF FAILURE PROBABILITY

The most efficient method for the calculation of the failure probability with human errors taken into

account seems to be the hazard scenario approach formalized in [6]. A hazard scenario is a more or less complex "scenario" of events. For example, an event in a scenario is a given set of human errors remaining in the design. Failure of the system due to failure in any of the hazard scenarios is failure of a series system, i.e. a system which fails if any of its links fail or in any of its hazard scenarios. Let F_i denote the failure event in scenario i, then

$$P_f = P\left[\bigcup_{\{N\}} F_i\right] \tag{12}$$

in which the union operation runs over all the events $\{N\}$. Let M_i be the set of errors in hazard scenario i, then the probability of the event F_i is the probability that only the set of errors $\{M_i\}$ remains in the design and failure occurs given the errors remain

$$P(F_i) = P(\{M_i\}\text{ remains})\,P(\text{failure}|\{M_i\}\text{ remains}) \tag{13}$$

The probability that only the errors M_i remain in the design is the probability that these errors have occurred and not been detected multiplied with the probability that no other errors remain. For each of the scenarios the probability of failure has to be calculated. This can be done by the available reliability methods such as FORM/SORM (see e.g. Madsen, Krenk and Lind [2]). Let X be a stochastic vector defining a reliability problem and let x be the outcome of this vector and e_i be the outcome of the vector E_i, which describes the set of errors in $\{M_i.\}$ The probability of failure is

$$P(\text{failure}|\{M_i\}) = \iint_{g(x,e_i)<0} f_X(x) f_{E_i}(e_i)\,dx\,de_i \tag{14}$$

where $f_{E_i}(e_i)$ is the joint density function of E_i, $f_X(x)$ is the joint density function of X and $g(x,e_i)$ is a limit state function defined in such a way that $g(x,e_i) < 0$ corresponds to failure. We consider a structural component where the load can be described by the stochastic variable S and the resistance by the stochastic variable R. A representative limit state function for this structural component is

$$g = R - S \tag{15}$$

The mean value of the resistance is determined according to eq. (2). The effect of the errors is introduced as

$$\varepsilon_i = \prod_{\{M_i\}} E_i \tag{16}$$

7. EXAMPLE

For the purpose of comparing the checking schemes the following simple example is considered. The resistance of the structural component is log normally distributed with mean $\mu_R = 3.158$ and coefficient of variation $V_R = 0.2$. The load is normally distributed with mean 1.0 and coefficient of variation $V_S = 0.2$. The reliability index of the error-free structural component is $\beta = 4.066$, which corresponds to $P_f = 2.89\ 10^{-5}$. The cost of failure of the error-free structure is $C_F = 20000$.

In table 1 the occurrence probabilities and magnitudes of the errors, which are included in the analysis, are given. The occurrence probabilities are those for a designer with the qualifications of a student. The calculation errors occur with the intensity $\lambda = 30.0$. Two load case errors are included in the example. The smallest of these (magnitude 0.85) is very likely to occur. The other load case error (magnitude 0.65) has a considerably lower probability of occurrence. There is enough time available to perform the design task with normal care, and the design task is performed under suitable working conditions.

Table 1: Probability of occurrence and magnitudes (LN denotes the logarithmic normal distribution).

Error	Probability	Magnitude
Geometry	0.025	LN(1.0;0.75)
Load 1	0.15	0.85
Load 2	0.03	0.65
Calculation	0.0136	LN(1.0;2.03)

Only three different levels of qualification of both designer and checker are considered. In table 2 the parameters which depend on the qualification of the checker and designer are shown. The values of p_{ED} and p_{EC}, the probability of making a design and concept error, respectively, in table 2 are the occurrence probabilities relative to the occurrence probabilities for a student (table 1). It is estimated that the probability of making a concept error decreases more rapidly with the experience of the designer than the probability of making a design error. It is assumed that t_D, the time necessary to perform the design task with normal care, decreases with experience of the designer, and that the cost per unit time increases with the experience. The relative increase of the cost per unit time, however, is judged to be smaller than the relative decrease of the time necessary to perform the design task. This implies that the cost of the design becomes smaller as the knowledge and experience of the designer increase. The checking efficiency a is assumed to be inversely proportional to the time t_D required to perform the design task.

Table 2: Parameters

A_D/A_C	p_{ED}	p_{EC}	t_D	$c_D = c_{OA}$	a
Student	1.0	1.0	120	1.0	0.075
Normal	0.3	0.1	60	1.5	0.15
Expert	0.1	0.01	30	2.0	0.30

SCHEME 1: The results for scheme 1 are given in table 3 for all three levels of qualification of the checker/designer.

Table 3: Optimum for scheme 1.

Designer	Checker	t_{OA}	C	P_f
Student	Student	29.0	217.0	0.00342
Normal	Normal	12.0	117.8	0.000491
Expert	Expert	5.5	73.5	0.000159

Because the efficiency of the check is high throughout the checking process the optimal checking time is relatively short, about 20 - 25 % of the time spent on the design. A designer/checker with the qualification of a student is likely to make concept errors. Therefore, the failure probability at optimum is more than 100 times larger than for the error-free structure. For the normal designer/checker and the expert the failure probability at optimum is 17 and 5.6 times larger than the failure probability of the error-free structure, respectively. This demonstrates, at mentioned earlier, that in order to use this scheme certain qualifications are required. Partly because of the low failure probability and partly because an expert performs the design at the lowest cost the total cost are also smallest when the designer/checker is an expert and increase with decreasing qualification of the designer/checker.

SCHEME 2: By scheme 2 the checker is always an expert. There are, however, no special qualifications required for the designer. The example is calculated for all three different levels of qualification of the designer. The results are given in table 4.

Table 4: Optimum for scheme 2.

Designer	Checker	t_{OA}	C	P_f
Student	Expert	14.2	152.1	0.000186
Normal	Expert	12.6	118.6	0.000174
Expert	Expert	11.0	87.3	0.000160

As expected the optimal duration of the check increases as the qualification of the designer decreases. The necessary checking time when the designer has the qualification of a student, however, is only 29 % larger than when the designer is an expert. The qualification of the designer has relatively little influence on the optimal checking time.

The qualification of the designer also seems to have little influence on the optimal failure probability. Because the differences between the optimal checking times and failure probabilities are small, the differences between the optimal cost for the three levels of qualification of the designer are almost solely caused by the differences between the cost of the design.

SCHEME 3: No special qualifications of either designer or checker are required by scheme 3, but a kind of negative correlation between designer and checker exists. The checking is often planned in such a way that the inexperienced engineer checks the calculation of the more experienced engineer. The calculations performed by the inexperienced engineer are checked by an expert, who is likely to detect the errors, which have been committed by the inexperienced engineer with large probability. The following three combinations of designer and checker are investigated (see table 5).

Table 5: Combinations.

Designer	Checker
Student	Expert
Normal	Normal
Expert	Student

The probability of a concept error remaining in the design depends on the degree of dependency between the designer and checker. Three different levels of dependency are investigated.

1. No dependency: The probability that the error remains is the product of the occurrence probabilities for the designer and the checker. The results are given in table 6.

2. Full dependency: The probability that the concept error remains is the minimum value of the probability of

occurrence for the checker and designer. The results are given in table 8.

3. Medium dependency: The mean value of the probabilities for fully dependent and no dependence. The results are given in table 7.

Table 6: No dependency

Designer	Checker	t_{OA}	C	P_f
Student	Expert	14.2	154.0	0.000180
Normal	Normal	24.0	130.6	0.000232
Expert	Student	40.0	105.9	0.000297

Table 7: Medium dependency.

Designer	Checker	t_{OA}	C	P_f
Student	Expert	14.2	154.1	0.000188
Normal	Normal	24.0	131.0	0.000250
Expert	Student	40.0	105.9	0.000298

Table 8: No dependency.

Designer	Checker	t_{OA}	C	P_f
Student	Expert	14.2	154.1	0.000189
Normal	Normal	24.0	131.4	0.000268
Expert	Student	40.0	106.0	0.000300

The duration of the check for concept errors and the efficiency of the check for design errors does not depend on the degree of dependency between designer and checker. This implies that the optimal duration of the check is also independent of the degree of dependency (see tables 6-8). As the dependency between designer and checker increases the probability that a concept error remains increases. Thereby, the total costs and the failure probability at optimum increase with increasing dependency (see tables 6-8).

The probability that a concept error remains is never larger than the probability that the best qualified of both checker and designer would have made the error. The designer and checker usually are chosen in such a way that either one is well qualified. This means that the probability that a concept error remains is small even though designer and checker are fully dependent. This again implies that the effect of the dependency is small. The effect of the dependency increases with increasing cost of failure. For larger cost of failure more time will be spent in order to detect design errors and the relative contribution to the total failure probability from concept errors becomes larger.

8. CONCLUSION

It might appear that the models selected are rather special and the systems are not general. Sensitivity studies not reported herein, however, showed that the numerical results and thus the conclusions are rather robust in their relative order with respect to changes in the models. In fact all numerical results should be interpreted in terms of an ordering scheme rather than by absolute values. If one accepts that judgement by such ordered values is reasonable the following main conclusions can be drawn.

The overall lowest cost are obtained by using scheme 1 with an expert designer/checker. In this case the total costs are 73.5 and the failure probability is only about 5.5 times larger than for the error-free structure. If the designer and checker were both experts and independent (scheme 2) about the same failure probability at optimum is found, but at a larger cost. In reality not all designers and checkers can be experts. If the designer has normal qualifications the total cost are about the same for scheme 1 and 2. The failure probability obtained by using scheme 1, however, is considerably larger than the failure probability obtained by scheme 2. Since society is risk adverse scheme 2 is preferable to scheme 1. If the designer has the qualifications of a student scheme 1 leads to unacceptable high failure probability and the overall largest cost. Also in this case scheme 2 is preferable.

For all levels of qualification of the designer scheme 3 leads to larger cost. Scheme 3, however, shows that the effect of dependence between designer and checker is small if only one has better than normal qualification.

From this example it can be concluded that for an expert designer the optimal choice of checking is scheme 1. For designers less qualified scheme 2 offers the best alternative. This, however, cannot be a general conclusion, because the optimum also depends of the complexity of the design task and the cost of failure. For more complex design tasks the probability of making a concept error becomes larger and, thereby, the independence between the designer and checker becomes more important. For more complex design tasks scheme 3 presumably always is to be preferred.

The above conclusions made on the basis of numerical results from a simple, yet representative, example are nevertheless conditioned in the sense that other factors such as the educational system, the system of professional qualification and the economic and juridical (civil and criminal) environment play an important role.

REFERENCES

[1] Lind, N. C., Human error in Structural Reliability, *Structural Safety*, 1, 1983, pp. 167-176.

[2] Madsen, H. O., Krenk, S., Lind, N. C., Methods of Structural Safety, Prentice-Hall, 1986, New Jersey.

[3] Matousek, M., Schneider, J., Untersuchungen zur des Sicherheitsproblem von Bauwerken, Institut für Baustatik und Konstruktion, Eidgenössische Technische Hochschule, Zürich, 1976.

[4] Melchers, R. E., Harrington, M. V., Human Error in Structural Reliability - I, Investigation of Typical Design Tasks, Civil Engineering Research Reports, Monash University, Report No. 2/1984.

[5] Nessim, M. A., Decision-Making and Analysis of Errors in Structural Reliability, The University of Calgary, 1983, Ph.D.-Thesis.

[6] Rackwitz, R., Human error in Design and Structural Failure, in: A. S. Nowak (Ed.) Modeling Human Error in Structural Design and Construction, Proc. of a Workshop Sponsored by the National Science Foundation, 1986, ASCE, New York, pp. 216-224.

[7] Stewart, M. G., Melchers, R. E., Checking Models in Structural Design, *Journ. Struc. Eng.*, 115, 1989, pp. 1309-1323.