

Working Toward Introducing Reliability Design

Shinsuke Sakai, Ph.D.*

1. Introduction

My main activities so far have been primarily in fields related to pressure vessels and piping, with very little crossover into the automotive industry. Recently, I participated in a NEDO project⁽¹⁾ related to on-vehicle hydrogen tanks for automobiles, which gave me the opportunity to learn about this type of activity. This exposure to activities in fields that I'd had little experience in beforehand helped me to become aware of issues and complications in this field. I feel that reliability design is a subject that cannot be avoided when it comes to considering the development of this field in Japan. Therefore, I have decided to summarize this topic in this paper.

The "Reliability Design" mentioned in the title is the key phrase here. I'd imagine that few people have considered the design of hydrogen tanks from the perspective of reliability design in the past. However, G.W. Mair from BAM in Germany has really emphasized the importance of introducing the concept of "reliability design" for pressure tanks such as hydrogen tanks⁽²⁾.

In the past, safety in terms of standards in the machinery field has often been secured through the safety factor. In the mechanical engineering field, there are opportunities to learn about the safety factor through lectures on the core academic field of "Material Mechanics." The definition of the safety factor as written in the textbook⁽³⁾ on material mechanics that I studied at the time was "Allowable Stress = Material Strength/Safety Factor," and I was taught that the safety factor is determined empirically. Safety factors based on this concept are called empirical safety factors or deterministic safety factors. While not all of the safety factors listed in today's standards in the machinery field may be determined empirically, it seems that the basic concept has not changed greatly since then. Design using safety factors is extremely simple and can be said to be a convenient method for both designers and regulators.

If the impact from the damage to a mechanical structure is not large, it is considered reasonable to perform safety management by using a simple deterministic safety factor like this. On the other hand, since enhancement in the performance of mechanical products has been sought after in recent years, there are limits on performing safety management with just a deterministic safety factor. For example, damage in the event of an accident may become more severe when enhancement in performance is pursued.

The concept of risk-based design, or reliability design, is important for rational design in these situations.

In this paper, I shall provide an outline on trends in related standards, applicable examples, current issues, and more, starting with introductory content so that even readers unfamiliar with reliability engineering will be able to understand. In addition, since the English expression for "Safety Factor" is "Safety Factor," it should really be called "Safety Coefficient," but since the term "Safety Factor" is also widely used, I've decided to use both terms in this paper without differentiating between them.

2. Tolerance Method Complications

The definition for allowable stress that I learned from lectures on material mechanics when I was a student was given as follows⁽³⁾.

$$\text{Allowable stress} = \frac{\text{Standard strength}}{\text{Safety factor}} \quad (1)$$

Safety is confirmed by evaluating stress in mechanical evaluation and confirming that the maximum stress does not exceed allowable stress. It was stated that the method for determining the safety factor is based on past experience. This concept of safety design is extremely simple, and the fact that it's easy for regulators to confirm safety can be said to be an advantage. If it's a simple mechanical structure, it's not practical to expend a great deal of effort on designing it, and it's thought that there is a rationality in adopting this level of design method.

However, various shortcomings may be exposed in safety factors determined empirically when the basis is not clear. Let's look at a few examples of this.

1. The size of the safety margin cannot be clearly stated since it's not clear which damage mode it's being designed for.
2. Even if attempts are made to rationalize the safety margin, it's challenging to provide an explanation linked to the basis.
3. The designer will not understand the incentive behind creating a better design if the basis for the safety factor is unclear.
4. The safety factor tends to be overestimated in methods for explaining safety using the safety factor, and it's not easy to lower the safety factor once it has been determined.

* Visiting professor, Yokohama National University

Table 1 Historical background on Sec. VIII safety factor reduction

Year	Details
1915	Code for power boiler, 1st ed.
1925	Sec. VIII, 1925 ed. Tensile strength safety factor set to 5.
1942/43	Safety factor reduced from 5 to 4 based on national request to secure strategic supplies (materials).
1998	Increase in requests to reduce the safety factor from 4 to 3.5, based on enhanced material performance and enhancement of standard specifics over past 50 years.

A high degree of safety is required in particular in cases like those where hydrogen tanks are installed in fuel cell vehicles, so it's thought that complications like these will become more prominent. Even now, it's thought that the safety factor in material mechanics is taught using nearly the same content. In addition, it's thought that the fundamentals of Japanese safety standards are based on the empirical safety factor. While a lot of mechanical structures may be realized through methods based on this type of tolerance method, rational safety margins should be optimized in the future in order to bring out top performance in mechanical products. It will be extremely important in these cases to introduce reliability design rather than the empirical safety factor.

One aspect of the safety factor can be understood by looking at the historical background of the values of the safety factor in the field of pressure vessels and piping, a field in which I've been deeply involved. Japan's design standards for pressure vessels refer to the standard of the American Society of Mechanical Engineers (ASME), the Boiler and Pressure Vessel Code. The design standards for pressure vessels in particular are specified in Section VIII, but around 1998, a dramatic change was made to reduce the safety factor for the tensile strength of material from 4 to 3.5. Looking at the literature⁽⁴⁾ that summarizes the basis for this provides a glimpse of a cross section of the characteristics of the safety factor. Table 1 summarizes the historical background on safety factor reduction based on the literature.

In 1915, boilers were in widespread use in the United States. In modern times, one rarely hears anything about large boiler accidents, but at that time, accidents involving fatalities were practically a daily occurrence in the U.S. Standardization for design standards was not in place at that time, and the need to do so in order to enhance the situation was recognized. This resulted in an opportunity that led to the publication of the first edition of the ASME standards. Sec. VIII, the standards for pressure vessels including boilers, was published in 1925, and the safety factor for the tensile strength of pressure vessels in use at that time appears to have been set at 5. There is no clear basis for this value, and it's assumed that it was set based on experience and opinions of people close to the project. Boiler-related accidents declined thanks to the standardization of boiler standards, and large boiler-related accidents caused by issues at the time of design were successfully avoided for

the most part thanks to the standards being revised further as time went on. However, the safety factor that had been established continued to be used without any changes in its value. This value was first reduced during World War II in 1942/1943. This was done based on a national request for the procurement of strategic supplies rather than for engineering reasons. As a result, the safety factor was reduced from 5 to 4, but this also made it possible to reduce the thickness of pressure vessels, allowing them to be utilized as strategic supplies. In other words, it was reduced through pressure in conjunction with a national request for reasons completely unrelated to engineering, demonstrating how ambiguous the safety factor value was. However, reducing the safety factor to 4 did not result in an increase in boiler-related accidents, and it remained unchanged for the next 50 years. However, if both material performance and the level of technical management increase and are reflected in the standards, accidents related to the design standards would no longer occur, and the industry would likely demand further reductions in the safety factor. In 1998, the safety factor was reduced from 4 to 3.5 based on a technical report⁽⁴⁾ published by the WRC. Along with verifying increases in the level of technical management in detail, increases in material performance were also verified through this report, but it does not appear that the basis for setting the safety factor value to 3.5 was clearly stated. Optimizing the safety factor based on experience like this is generally applicable for mechanical products as well and could be called a widespread concept in the machinery field.

There are no complications with the tolerance methods themselves, which are based on the empirical safety factor. It's important to use them appropriately to address the complications for which these methods are applied, and complications will be exposed if they are not used appropriately. In fact, it's considered that there have been no major complications with most of the mechanical products made by design standards based on the empirical safety factor in the past. It's clearly not efficient to exert a great deal of effort to make a strict design even for design for normal use range, and in this case, the application of the tolerance method could be called appropriate. However, challenges accompany this when addressing things through the empirical safety factor when there's a desire to operate under extreme conditions to bring out the performance of a mechanical product, or when it's necessary to help

ensure high reliability in light of the severity of an accident. It's desirable to clarify the limit state for exhibiting the performance of a mechanical product and to design it with the distance between operating conditions and the limit state (in other words, the safety margin) as the management target. This is precisely the concept of reliability design. It's important to use the tolerance method and reliability design appropriately depending on the application in question.

3. Definition of Reliability Design

3.1. Concept of Reliability Design

The words of the Russian playwright Anton Chekhov (1860–1904) are quoted at the beginning of G.W. Mair's book, and I referred to these in the process of learning about trends in the stochastic treatment of on-board hydrogen tanks.

There is no certainty(safety),
only different degrees of uncertainty(danger).
Anton Pawlowitsch Tschechow (1860–1904)

Along with symbolizing the essence of books, these words also express the essence of reliability design. My personal interpretation would be, "There is no such thing as safety (as defined by the tolerance method), only different degrees of danger." The method for evaluating this degree of danger is reliability engineering, and the method for designing according to these results is reliability design.

In Fig. 1, Chekhov's words have been visualized as an engineering conceptual diagram. The upper half shows the tolerance method, or deterministic method, widely used in the traditional mechanical engineering field. In this method, tolerance is set based on the empirical safety factor. It's judged to be dangerous if stress rises even a little bit above the tolerance and safe if it falls even a bit below the tolerance. In other words, the judgment is either/or. On the other hand, the lower half of the figure shows the conceptual diagram for the stochastic method used in reliability design. There's a wide gray zone between safety and danger; therefore, it's not an either/or judgment. This gray zone is the area expressed by the "different degrees

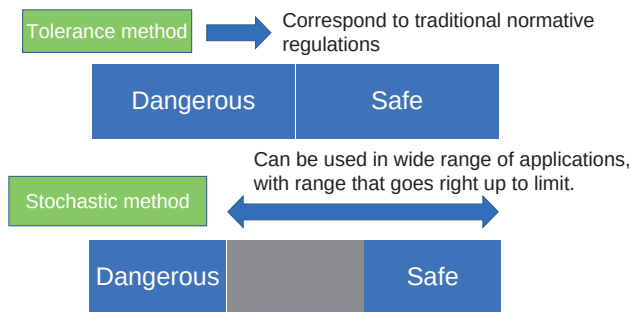


Fig. 1 Differences between stochastic design method and allowable stress method

of uncertainty (danger)" in Chekhov's words. When it is in this area, decisions are made based on evaluations without judging whether it's safe or dangerous. If it approaches danger, it's necessary to make an effort to shift it even a little bit toward safety, but usage is permitted once that effort has been made. Accordingly, as it should be clear from the comparison with the tolerance method, the usable range is expanded based on the premise of performing evaluation. Representative examples of evaluations are reliability evaluation and risk evaluation. Design based on reliability evaluation is called "reliability-based design," and design based on risk evaluation is called "risk-based design."

Figure 2 shows a conceptual diagram for decision-making in risk-based engineering that corresponds to Fig. 1. The horizontal length of the inverted triangle shown in the center indicates the size of the risk being evaluated. In other words, the top end shows where risk is the largest, and the bottom end shows where there is zero risk. To clarify the contrast between the risk method and tolerance method, the risk method is shown to the left of the triangle, and the tolerance method is shown to the right. In the case of the risk method, judgment for decision-making is divided into the three areas formed by the black lines. The uppermost area is where the risk value is excessive and unacceptable, while the lowermost area is the area where the risk value is sufficiently small and widely acceptable. The intermediate area is tolerable and acceptable, but it's necessary to make an effort to reduce the risk as long as it remains in this area. The risk values that divide these three areas are set as appropriate depending on the equipment subject to evaluation and the usage environment. This concept is called "As Low As Reasonably Practicable (ALARP)" and is a concept proposed by the British Health and Safety Executive (HSE). This concept is one widely used as a method for making risk-based engineering decisions. This intermediate area corresponds to the gray zone in the bottom row of Fig. 1 and is also called the ALARP area.

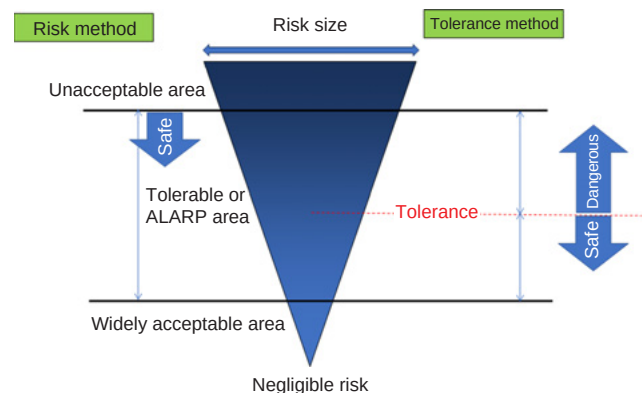


Fig. 2 Concept of decision-making for risk-based engineering

Based on recognizing that there's risk associated with most machines, efforts to reduce risk are required for machines included in the ALARP area. According to the definition from ISO Guide 73, areas below the ALARP area are judged to be safe. On the other hand, in the case of the tolerance method on the right side, judgment on whether it's safe or dangerous is performed by either/or when it's beyond a certain tolerance. In these cases, compared to the risk method, the area that is treated as safe is narrower, but various complications arise in conjunction with this. First of all, if it's judged to be "safe," it's natural that there will be less awareness for shifting to the safer side in response to that result, and there may be no effort to do so at all in some cases. On the other hand, under the risk method, effort to reduce risk is required as long as it is within the ALARP area. Next, if it's judged to be "dangerous" under the tolerance method, then it will never be accepted no matter how much effort is put forth. Under the risk method, if something is within the ALARP area, it will be accepted by reducing the risk. In other words, designers are rewarded for their efforts. However, in the case of the risk method, risk evaluation is required for decision-making in contrast to the tolerance method, and there's no denying that a lot of effort and labor are necessary.

The concept of reliability design will be explained using a simple RS model in which the only design variables are strength (R) and load (S). If R and S vary, the contour lines of the probability density function on the RS plane will be concentric ellipses, as shown in Fig. 3. The position of the vertex of the probability density function corresponds to the mean value of two random variables. What's important in reliability design is to quantitatively show how much of a safety margin there is rather than to judge safety in terms of black or white. To do this, it's necessary to clearly indicate the damaged area in Fig. 3 and to investigate its relative relationship with the state of distribution for RS . The limit state function $g(R, S)$ is defined for this reason. An area where this function is negative indicates damage, and one where it's positive indicates that it is undamaged.

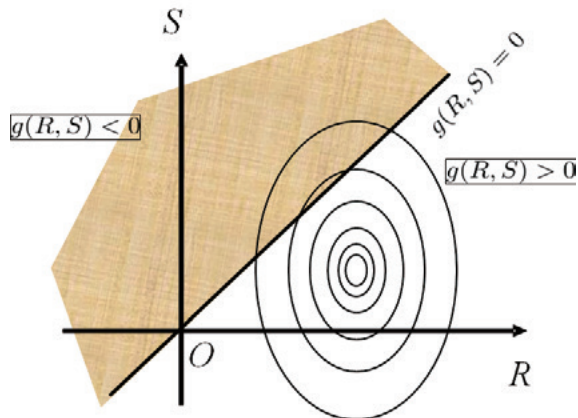


Fig. 3 Reliability design concept explanatory diagram

The boundary line where this is 0 is called the "limit state curve." In other words, it's defined by Eq. (2).

$$g(R, S) = R - S \quad (2)$$

The part indicated with brown hatching area in the figure is the damaged area, and how easily damage may occur can be found by examining how far the limit state curve that is the boundary line for the damage is from the position of the mean value of R and S . The Advanced First Order Second Moment Method (AFOSM) is a method to quantitatively derive the safety margin from the limit state function and the statistical properties of each design variable.

The method of evaluating reliability based on the limit state function in this fashion is called the "limit state function method," and it would be good to briefly explain the significance of this method. As shown in Fig. 3, processing is simple when the only design variables are strength (R) and load (S), but this alone is not sufficient when aiming for a higher degree of design. The first complication is that the design variables that should be considered may include a variety of other variables aside from strength and load, such as dimensions, surface roughness, thickness reduction rate, internal pressure, weight, stress, and displacement. In this case, a general reliability evaluation method for multiple variables is required. The second complication is that the definition of limit state is that there can be many different ones, depending on the interest of the evaluator. In the case of Fig. 3, the physical limits of the damage are defined as the limit state, but in addition to this, some evaluators may be interested in the margin for the standard limit values. In addition, when there are multiple damage modes, it becomes necessary to set a limit state for each different damage mode. The limit state function method is a method that can be used to respond flexibly to these complications. In the limit state function method, limit state function $g()$ is defined as follows.

$$\begin{aligned} Z_i = g_i(X_1, X_2, \dots, X_n) > 0 &\Rightarrow \text{Damage Mode } i \text{ does not occur} \\ &\leq 0 \Rightarrow \text{Damage Mode } i \text{ occurs} \end{aligned} \quad (3)$$

There's no limit to the number of design variables ($X_1, X_2, \dots, X_n$), and Damage Mode i may be defined according to the designer's interests. An example of setting the limit state function is shown below.

$$\begin{aligned} \text{When interested in maximum stress: } g &= \sigma_{\text{limit}} - \sigma_{\text{max}} \\ \text{When interested in maximum displacement: } g &= \delta_{\text{limit}} - \delta_{\text{max}} \\ \text{When interested in standard limit pressure: } g &= p_{\text{code}} - p_{\text{working}} \end{aligned} \quad (4)$$

In this way, the limit state function method is a versatile, efficient reliability evaluation method, but its handling method is complicated, and there is an issue that it's challenging for general designers to understand. For example, if there are two design variables, as shown in Fig. 3, drawing can be done in two-dimensional space and is easy to understand intuitively. However, when there are three variables, it shifts to three-dimensional space, as

shown in Fig. 4, and if the function shape is complex, the limit state surface will be complicatedly curved, making it challenging to understand intuitively. If the number of variables increases beyond this, then it would need to be handled in a multidimensional space, making it even more complex. However, although strict handling of reliability evaluations like this may be necessary at the researcher level, designers and standards users do not necessarily need to master these techniques. For example, for the Partial Safety Factor Method, which incorporates reliability design into standards, reliability design is achieved by simple evaluation through simple calculations using a partial safety factor table prepared in advance based on reliability theory. The specifics of this will be explained in the next chapter. Therefore, familiarity with all aspects of reliability theory is not necessary to practice reliability design in the industry, there are cases where individuals would like to learn the fundamental theory behind it, so reference materials have been listed in the literature⁽⁵⁾⁽⁶⁾⁽⁷⁾.

3.2. Partial Safety Factor Method Definition

The cutting edge of reliability engineering is performing strict evaluations after defining the limit state function indicated by Eq. (3), but in addition to specialized knowledge, designers also need a lot of effort and time to program and perform these evaluations for each design. To address this complication, a partial safety factor table is placed in the standard, allowing for simple reliability design to be achieved by a simple evaluation through simple calculations. The conceptual treatment is described below.

If $X_1, X_2, \dots, X_n$ are random variables, then variable Z evaluated through Eq. (3) is also a random variable. If the probability density function of Z is as shown in Fig. 5, then $Z = 0$ is the limit state and the area where $Z < 0$ is the damaged area, so the area of the blue part in the figure is

damage probability (P_f). Various quantitative evaluations may be performed using P_f , but generally, it will be an extremely small value like 10^{-6} . Therefore, the reliability index (β) is often used. In Fig. 5, the distance between the mean value of Z (μ_Z) and limit state $Z = 0$ is an index for the safety margin. The standardized value derived from dividing this distance by the standard deviation of Z (σ_Z) is called the reliability index. β is often used as the symbol for the reliability index. During normal distribution of the random variables of design variables, the distribution of Z is often close to normal distribution as well, the following approximation relationship forms between P_f and β , and there is a one-to-one correspondence relationship.

$$P_f = \Phi(-\beta) \quad (5)$$

Here, $\Phi()$ is the standard normal cumulative distribution function. For example, in the field of architecture, values of $\beta = 2, 3$, etc. are set as reliability to be targeted (target reliability), and the partial safety factor table corresponding to them is provided in the standard. For example, for target reliability β_0 , if partial safety factors $\alpha_1, \alpha_2, \dots, \alpha_n$ for $X_1, X_2, \dots, X_n$ are prepared in advance by a reliability expert, then checking whether the design values $X_1, X_2, \dots, X_n$ set by a designer satisfy target reliability β is performed as follows.

$$\begin{aligned} g(\alpha_1 X_1, \alpha_2 X_2, \dots, \alpha_n X_n) > 0 &\Rightarrow \text{Satisfies target reliability } \beta \\ g(\alpha_1 X_1, \alpha_2 X_2, \dots, \alpha_n X_n) \leq 0 &\Rightarrow \text{Does not satisfy target reliability } \beta \end{aligned} \quad (6)$$

If evaluated at this level, it could be handled by processing through simple calculations even with a designer unfamiliar with reliability engineering.

However, there are some precautions to keep in mind when using a partial safety factor table. When reliability design is performed with rough approximations, it is a simple and convenient method relative to strict reliability evaluation, but consideration should be given to its ease of use in terms of practicality. Now, let's imagine that we've

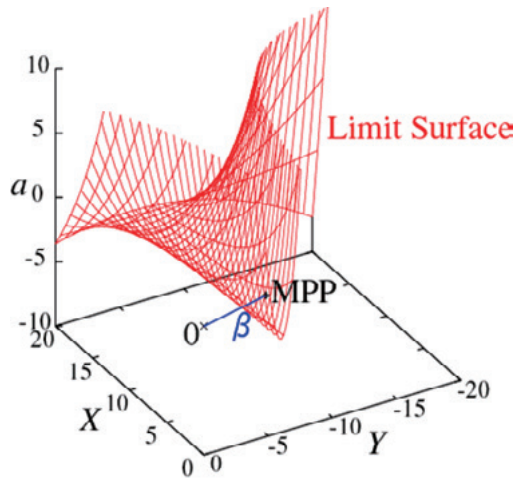


Fig. 4 Limit state curve when there are three random variables.

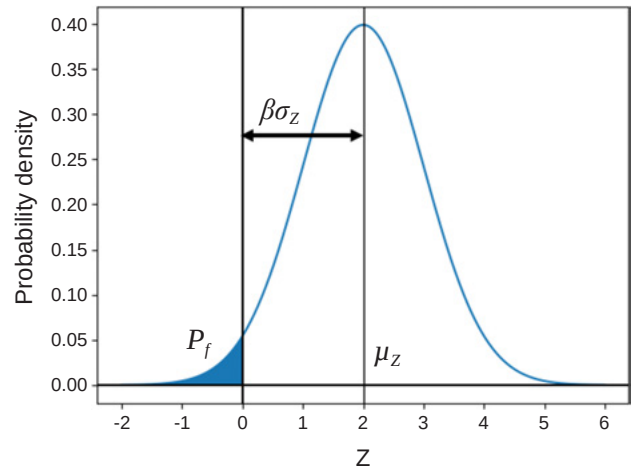


Fig. 5 Reliability index concept

Table 2 Example of complex partial safety factor table

Probability offailure	$a_0 < X_1 < a_1, b_0 < X_2 \leq b_1$				$c_0 < X_4 < c_1, d_0 < X_7 \leq d_1$			
	α_1	α_2	...	α_n	α_1	α_2	...	α_n
$P_f = 10^{-2}$ ($\beta = 2.0$)	1.1	2.5	...	3.8	1.3	1.1	...	1
$P_f = 10^{-3}$ ($\beta = 3.09$)	1.4	2.3	...	3.4	1.5	1.2	...	1
$P_f = 10^{-6}$ ($\beta = 4.75$)	1.6	2.1	...	3.2	1.9	1.3	...	1

Table 3 Role allocation for partial safety factor table development

Person in charge	Role	Description
Researcher	Develops physical models for target concerns and derives limit state function.	Advanced comprehension of limit state design methods is required.
Standards developer	Creates new partial safety factor tables for target concerns.	Comprehension of limit state design methods is required.
Standards user	Appropriate comprehension of partial safety factor tables is required.	Comprehension of details of limit state design method is not necessarily required, but being able to correctly understand how to read and evaluate table is required.

been given a partial safety factor table like Table 2 when there are n number of design variables.

Numerical values for the corresponding partial safety factors $\alpha_1 \sim \alpha_n$ are picked up according to the target reliability shown in the leftmost column. However, when the limit state function is non-linear and complex, the partial safety factor values may also change sensitively depending on the area of application. As a prerequisite for the Partial Safety Factor Method, they should be applied within a region where the partial safety factor value is almost constant. Therefore, it is necessary to investigate areas where the partial safety factor is almost constant and to set partial safety factors for each identified area, as shown in the top row of Table 2. Furthermore, since these values need to be calculated each time for target reliability, it's conceivable that the partial safety factor table corresponding to all of these would be complex. This needs to be enhanced from the perspective of practicality. An effective solution for this would be to calculate the sensitivity to the damage probability for each random variable. This sensitivity can be calculated easily using the limit state function method. Please refer to the literature⁽⁵⁾⁽⁶⁾⁽⁷⁾ for details. The random variables that should actually be targeted can be narrowed down through sensitivity analysis. For example, in the case of a partial safety factor table created⁽⁸⁾ for evaluating the reliability of localized thinning of pipe walls, in contrast to the nine random variables for the limit state function, the variables can be narrowed down to only the three that are sensitive to damage probability. In this case, the partial safety factor table could be made for only the three random variables, simplifying it and making it convenient in terms of practicality.

3.3. Role Allocation Between Industry and Academia for Reliability Design Promotion

A high level of specialized knowledge is required for making full use of the limit state design methods used in reliability design. Accordingly, it's not realistic for pure standards users to perform evaluations using the limit state design methods every time a design is created. Therefore, there is the Partial Safety Factor Method as a means of listing it in the standard, but the issue is the process for developing the partial safety factor table. This is where cooperation between reliability researchers, standards developers, and standards users is considered to be important. Examples of this allocation of roles are shown in Table 3. Among these, it's conceivable that roles could be allocated in such a way that universities and research institutes would be responsible for the researchers; industry and academia would both be responsible for developing standards; and the resulting product, the partial safety factor table, would be utilized by industries that use the standards.

4. Examples of Safety Factor Relaxation

As mentioned in Chapter 2, safety factors listed in standards have been amended due to various factors. This has not been done on the basis of scientific grounds, and social demands are considered to be one factor behind this. Safety factor optimization has been performed in a number of industrial fields in the past, even in Japan. I'll introduce two examples here to contribute to future investigation of safety factor optimization.

4.1. Introduction of Maintenance Standards for Pressure Equipment

Design is performed at the design stage for mechanical products in consideration of the safety factor written in the design standards. When devices designed and manufactured based on the design standards are added at the in-service stage for pressure equipment in plants, such as those in the nuclear power field, chemical industry, or oil refining industry, the standards for maintaining those are separate from the design standards and are called maintenance standards. Representative examples of these include the standards for the nuclear power field published by the Japan Society of Mechanical Engineers⁽⁹⁾ and standards related to pressure equipment published by the High Pressure Institute of Japan⁽¹⁰⁾⁽¹¹⁾. Maintenance standards for the nuclear power industry were first established in 2000⁽¹²⁾, but operational standards for maintenance standards did not exist before that, and Japan's concept of safety regulations has placed emphasis on the design stage, or design standards, for a long time. When securing safety for the maintenance stage according to the design standards, it's necessary to "maintain the state at the time of installation even if the state at the time of production is the in-service stage." However, mechanical equipment deteriorates over time. This has created a gap between safety maintenance practices and the spirit of legal compliance, and contradictions have surfaced in terms of the intention behind safety maintenance practices being contrary to the law. When looking at this from the safety factor perspective at the design stage in particular, not all information on design is collected, so the design is based on predictive behavior, and the safety factor should be set high to secure the safety margin. However, at the in-service stage, actual data is collected from the operation of the mechanical product, and the data predicted during design can actually be confirmed as well. Therefore, even if the safety factor is set excessively high at the design stage, it does not necessarily need to be operated at the same safety factor level at the in-service stage. In this way, the safety factor concept exists at both the design stage and the in-service stage, but the idea that the two numerical values do not need to be the same is firmly established. To clarify this distinction, for the nuclear power standards of the American Society of Mechanical Engineers (ASME), "Design Factor" is the term corresponding to safety factor used at the design standard stage, while "Structural Factor" is used at the in-service stage. It took 30 years from the time when maintenance standards were established by the ASME until maintenance standards were established in the nuclear power field in Japan.

Even though the introduction of maintenance standards will ease the safety factor, there are three important elements for that. Those three pillars are "investigation," "evaluation," and "repair/replacement." Investigations were conducted periodically even prior to the introduction of maintenance standards, but the act of evaluation

was missing. When damage such as loss is detected, the harmfulness of that damage is evaluated through mechanical investigation, etc. If soundness is confirmed by the results from the evaluation, it is permissible to continue operating with some loss remaining. "Evaluation" regulations were published in 2000, "investigation" regulations in 2002, and "repair/replacement" regulations in 2004.

4.2. Introducing the Limit State Design Method to Mobile Crane Structure Standards

Around 2007, based on a request I received from the Japan Crane Association, I became involved in introducing the limit state design method to mobile crane structure standards. A mobile crane is shown in Fig. 6. The key to enhancing performance is to make it longer through weight reduction. Originally, Japan's advanced development technology for high-tensile steel should have had an advantage from the perspective of weight reduction, but in reality, Japanese manufacturers were at a disadvantage in international competition. The reason for this is that in Japan at that time, only allowable stress design methods were permitted under the mobile crane structure standards, while under the ISO standards⁽¹³⁾⁽¹⁴⁾ in Europe, it was possible to choose either the allowable stress design method or the limit state design method. Trying to make mobile cranes longer increases the risk of buckling and the amount of bending deformation. Therefore, it's important to achieve lengthening while being more aware of the limit state. Since there are limits in responding to the limit state under the allowable stress design method that's based on elastic design, Japanese mobile crane manufacturers were at an extremely disadvantageous position in terms of international competitiveness. Therefore, the task was given to incorporate the limit state design method into Japan's structural standards.

It was no easy task for Japan to develop an understanding for the introduction of the unfamiliar limit state design method, and no results were obtained despite a lot of time and effort being spent on this. As a result, when the ISO standards system was investigated, it was found that a standard regarding the general principles of reliability⁽¹⁵⁾ does exist as a standard that serves as the basis for mobile crane standards⁽¹³⁾⁽¹⁴⁾. On the other hand, the situation in Japan was that there were no corresponding JIS standards. It was expected that if corresponding JIS standards could be developed, then standards where the limit state function method is applied could be developed for each industry based on them, and that they would proliferate quickly. Therefore, appeals were made to related industrial fields and academic experts, and activities for the development of JIS standards were performed as a study group and subcommittee activity for the Japan Society of Mechanical Engineers. Ultimately, the High Pressure Institute of Japan became a development organization and JIS B9955:2017 was published⁽¹⁶⁾. The chapter structure of the JIS standards

is shown in Table 4. As shown in Chapter 5, the limit state design method was set as the basic concept, and the Partial Safety Factor Method is assumed to be applied as shown in Chapter 9. The mobile crane structure standards were revised in 2018, enabling designers to choose the most appropriate method (either the “allowable stress design method” or the “limit state design method”) according to the usage of the crane, etc. When there’s a desire to bring out the performance of a mechanical product with a stronger awareness of the limit state, it may not be possible to achieve it under the existing “allowable stress design method” from the perspective of the safety factor. The mobile crane structure standards could be called an example of a complication resolved by introducing the “limit state design method.”

Table 4 JIS B 9955 Chapter Structure

Chapter 1	Scope of application
Chapter 2	Terms and definitions
Chapter 3	Symbols
Chapter 4	Requirements and concepts
Chapter 5	Principles of limit state design
Chapter 6	Basic variables
Chapter 7	Analysis models
Chapter 8	Principles of design based on probability
Chapter 9	Design through partial factor method
Chapter 10	Evaluation of mechanical products during in-service period



Fig. 6 Example of mobile crane (photo provided by KOBELCO Construction Machinery Co., Ltd.)

5. Importance of Stochastic Treatment

In the past, I've participated in activities to develop standards in a large number of fields, and my overall impression is that stochastic treatment is only used in a limited number of cases. Deterministic treatment is used the majority of the time. Considering the importance of bringing out the performance of mechanical products in a state closer to the limit state, the introduction of stochastic treatment may be inevitable in the future. This is considered to be the case in the automotive field when considering installing high-pressure hydrogen tanks in fuel cell vehicles. I'd like to share two things I've noticed from my past experiences.

The first is my experience in fields related to nuclear power. When looking only at Japan, it's hard to see where country stands in this field, and I developed a strong awareness of this complication while taking part in an international workshop related to nuclear power. The workshop, titled "Forging a New Nuclear Safety Construct" (Washington DC, December 4–5, 2012), was held by the American Society of Mechanical Engineers (ASME) following the Fukushima Daiichi nuclear power plant accident. While the specifics of this workshop are described in the literature⁽¹⁷⁾, the purpose was to discuss a report published by ASME titled "Forging a New Nuclear Safety Construct" with individuals in leadership positions in the global nuclear power community. In this report, a new direction called the All Risk Approach was introduced as a direction for nuclear power in the future, and session moderator Kenneth R. Balkey asked me to report on the situation in Japan and to give my opinion on the matter. I explained that progress in Japan is slow, with little activity in terms of either a stochastic approach or a risk approach. In response to this, my recollection is that Mr. Balkey said something to the effect of, "Just as I thought. That's the Japanese mindset." At that time, I became painfully aware that this is how Japan is viewed by those outside of the country. In light of the importance of this report to the future of Japan's nuclear power field, I took part with other volunteers in completing the translation work, and the final product was published on the home page of the Japan Society of Mechanical Engineers⁽¹⁸⁾. However, looking at the situation since then, it's worrisome that it does not appear to have been fully utilized. I believe that risk-based engineering thinking and stochastic thinking will be extremely important in the future when considering how to bring out the performances of mechanical products through awareness of their limit states.

The second example is handling uncertainty when dealing with smaller samples of statistics. In these instances, in addition to the statistical properties of populations of random variables, it's necessary to handle the uncertainty known as the confidence level in English. While the term "confidence level" is used in the reliability terms in the JIS standards, etc., my personal opinion is

that this translation is not appropriate. If the English term "confidence level" is used for "confidence level" when translating the English term reliability as "reliability," some may confuse it with the English term "reliability." However, the two concepts are quite different. Perhaps reflecting this situation, there are instances where the confidence level is not handled in the standard, or is handled incorrectly. While this is common sense to those familiar with statistics, it's an unfamiliar concept to those involved in engineering, and I feel that it's necessary to reconsider it, including our educational methods. For example, consider a case where the allowable stress value for tensile strength is determined in association with reliability. If the tensile strength has normal distribution and if the mean value and standard deviation (its parameters) are known, then the probability density function could be plotted as shown in Fig. 7. In this case, if there was a desire to determine allowable stress so that it would result in reliability R , it could be determined as the stress value S_A at the location of Point A in the figure. Here, Point A is determined as the position where the probability that the tensile strength will be less than or equal to S_A is $1-R$. The value of $1-R$ is the area of the blue section in the figure, which is nothing but the probability of damage when the tolerance is set to S_A . However, in order to investigate the statistical properties of material strength, evaluation should be performed based on a finite number of samples (n). In this case, uncertainty accompanies the evaluation of the population. For example, the mean value and standard deviation, which are the parameters of normal distribution, will have a large degree of uncertainty if number of samples (n) is small. That uncertainty depends on n . Once the uncertainty has been taken into consideration, it will be necessary to give a value for the confidence level in order to determine the tolerance. An example of the tolerance for the U.S. MIL standards is

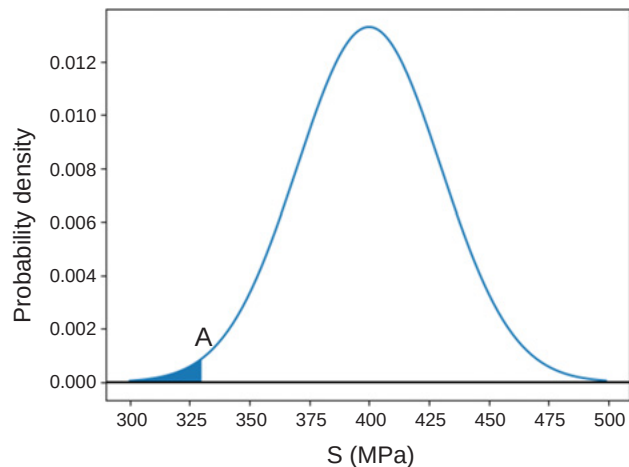


Fig. 7 Probability density function for tensile strength

Table 5 Examples of tolerance for MIL standard military aircraft

	Reliability	Confidence level
A-basis	99%	95%
B-basis	90%	95%

shown in Table 5 as a typical example adopted in the standards. Also, please refer to the explanatory article for technical details related to the handling of confidence levels⁽¹⁹⁾. When considering safety standards for hydrogen tanks, it may be challenging to secure the number of samples required for burst testing, so the complication with uncertainty related to small sample sizes may arise in these cases as well. In the next chapter, I will go over the method that G.W. Mair suggests for introducing a confidence level to manage this issue.

6. Safety Margin Optimization Concept

A high degree of safety is required for hydrogen storage tanks for fuel cell automobiles since they're used at high pressure levels. That said, it's preferable to avoid an excessive safety margin, so optimization is required. With hydrogen tanks, it's not possible to set up a large number of sample burst tests based on safety standards due to cost considerations. Therefore, as stated in the previous chapter, the uncertainty associated with small sample sizes needs to be handled. Since a high level of safety is required, it's natural to start with products designed and manufactured with a high safety factor as a starting point. G.W. Mair of BAM's concept⁽²⁾ could be helpful when considering optimizing the safety factor in situations like this, so I'll introduce it briefly here. First, he suggests the application of a Monte Carlo simulation as a countermeasure for being unable to secure enough samples. Monte Carlo simulation refers to generating the value of a specific random variable using random numbers, applying the value generated to the evaluation subject, and giving consideration to the phenomenon. The principle is extremely simple, and since evaluation can be completed sufficiently even on a stock PC, it's fair to say that it's an effective method for supplementing burst testing. For example, Fig. 8 shows the results from evaluating pass/fail judgment for burst testing under the ISO 11119-3⁽²⁰⁾ standards through a Monte Carlo simulation. The horizontal axis shows the standard deviation, while the vertical axis shows the mean value, and both are standardized by the maximum service pressure (MSP). The specimens are judged to have passed the test if all three of them exceed the tolerance of 2.5 and are judged to have failed it if any of them are below that. Pass/fail judgment tests are conducted on three specimens at a time, and the results are shown for 100,000 tests. The value in yellow is

the population value, and the mean value for groups of three and the standard deviation have a large amount of variation, as shown here. Also, the points in red show ones that failed the test, while the points in black show ones that passed. In this case, 59% are indicated as "passed." The ratio of ones that passed is called the Acceptance Ratio (AR). When the safety margin for tanks is excessive, it's only possible to get a 100% pass rate, and it's unlikely to see the size of the safety margin. The introduction of an index like the AR is considered to be helpful for visualizing the safety margin. When optimizing the mean value and standard deviation for the burst strength of hydrogen tanks from the perspective of the safety margin, a contour line for the AR values, which are combinations of the various mean values and standard deviations from the population, is effective. An example of a figure drawn like this is shown in Fig. 9.

G.W. Mair calls this figure an ISOASFALIA. The red line is the ISOASFALIA, and the values on the line are the AR values. Also, the boundary line for a reliability level of $1 - 10^{-6}$ is indicated by the black line in this figure. This

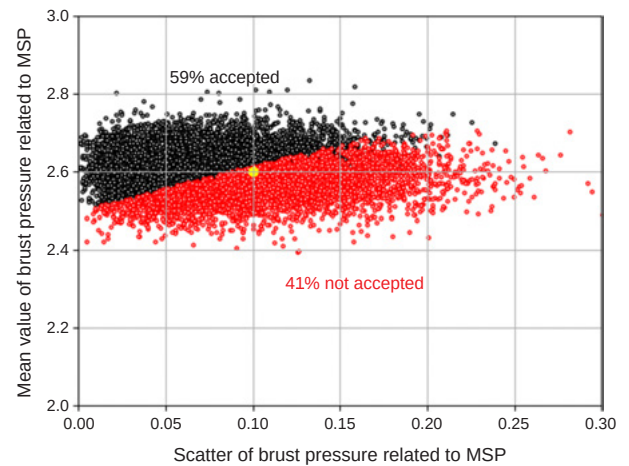


Fig. 8 Evaluation through Monte Carlo method for standard pass/fail

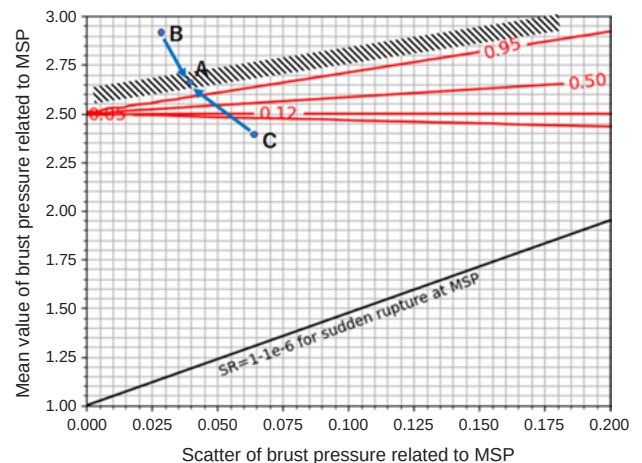


Fig. 9 Example of ISOASFALIA application

figure can be used to consider the safety margin while also considering the targeted reliability and the uncertainty of the small sample size.

For example, the concept of safety factor optimization is shown conceptually in Fig. 9. Imagine that the dashed line area is set as the optimization range in consideration of the AR values, and that among those, Point A is determined to be the target value. On the other hand, if we imagine the current value to be Point B, then shifting from Point B to Point A would be the optimization process. It's also conceivable that a great deal of effort and time would be required to reduce the margin from the excessive safety margin of Point B and shift to Point A. In cases like this, starting from a point with a smaller safety margin like Point C and moving closer to Point A might serve as a shortcut. In this way, this is considered to be an effective method for investigating the safety margin by visualizing various statistics.

7. Complications with Introducing Reliability Design

Finally, based on my experience, I would like to give my opinion on complications with introducing reliability design as a new phenomenon for industries. As shown in Fig. 10, I think that there are three major complications. Needless to say, the first of these is formulating standards and criteria. These should be officially recognized and formulated with international harmonization taken into consideration as well. When viewed from the perspective of stochastic treatment, I often feel that the current situation is still insufficient. The next important complication is the development of the databases required for carrying out various statistical considerations. I believe that developing databases on a public basis rather than keeping them confidential within specific organizations is important for the development of industry. With regard to this, in Japan, usage is often limited to within specific organizations, and this is an area where enhancement is desired. The final

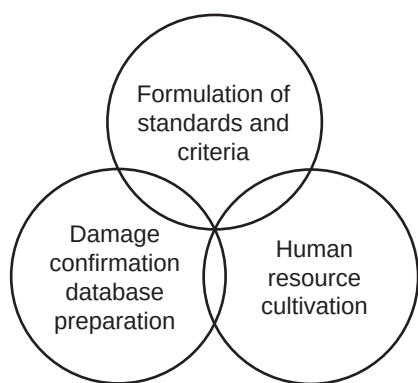


Fig. 10 Important elements for introduction of reliability design

complication is the cultivation of human resources involved in these fields. One thing that could be considered to be an effective means would be the introduction of a qualification authentication system. For example, the High Pressure Institute of Japan employs a system for “risk management engineer certification for equipment, etc.” to cultivate human resources involved in maintenance at plants, and the number of risk management engineers has grown dramatically with the start of this system. Cooperation between universities with specialized knowledge and industries would also be an effective means. In any case, I think that it's extremely important for industry to take the lead in moving forward on this.

8. Summary

Using on-board hydrogen tanks as the subject matter, I've presented the concept of reliability design, which is considered to be important to introduce in the future. In particular, I summarized my impressions from the perspective of someone from a different field. Based on my past experience, I also mentioned examples of reliability design and complications specific to Japan. In the future, it's believed that it will become extremely important to introduce reliability design once the limit state has been clarified further in order to bring out performance in mechanical products. This cannot be avoided, especially when considering optimizing the safety factor. Finally, I've summarized what are, in my personal opinion, the complications with introducing reliability design into industrial fields. I hope that this will prove useful as a reference.

Acknowledgements

Some of these results were obtained as a result of work commissioned by the New Energy and Industrial Technology Development Organization (NEDO) (JPNP20003). I would also like to thank Mr. Shigemitsu Kihara of BESTMATERIA Co., Ltd. for providing related materials.

References

- [1] https://www.nedo.go.jp/activities/ZZJP_100182.html, (2023/6/29)
- [2] G. W. Mair, 'Safety Assessment of Composite Cylinders for Gas Storage by Statistical Methods', Springer International Publishing, AG 2017, DOI: 10.1007/978-3-319-49710-5.
- [3] Udoguchi, T., Kawada, Y., Kuranishi, M.: Zairyo Rikigaku, SHOKADO, (1973) (in Japanese)
- [4] Evaluation of Design Margins for Section VIII, Div. 1 and 2 of the ASME Boiler and Pressure Vessel Code, WRC Bulletin 435, September (1998).
- [5] Achintya Haldar and Sankaran Mahadevan, 'Probability, Reliability and Statistical Methods in

- Engineering Design', John Wiley & Sons (2000), ISBN: 0-471-33119-8.
- [6] Thomas A. Cruse, 'Reliability-Based Mechanical Design', MARCEL DEKKER, INC. (1997), ISBN: 0-8247-9793-0.
- [7] Isaac Elishakoff, 'Safety Factors and Reliability: Friends or Foes?', Kluwer Academic Publishers (2004), ISBN: 1-4020-1779-0.
- [8] Sakai, S., Iwasaki, A., Sasaki, T., Miyazaki, S., Ishizaki, Y., Kaida, T.: Development of Partial Safety Factor Table for Reliability Assessment of Local Metal Loss, Journal of High Pressure Institute of Japan, Vol. 57, No. 2, p. 66-72, (2019)
- [9] The Japan Society of Mechanical Engineers (JSME): Code for Nuclear Power Generation Facilities -Rules on Fitness- on Fitness-for -Service for Nuclear Power Plants-, JSME SNA1-2020, (2020)
- [10] High Pressure Institute of Japan: Assessment Procedure for Crack-Like Flaws in Pressure Equipment - Level 1, HPIS Z 101-1: 2008, (2008)
- [11] High Pressure Institute of Japan: Assessment Procedure for Crack-Like Flaws in Pressure Equipment - Level 2, HPIS Z 101-2: 2011, (2011)
- [12] Kashima, K.: Genshiryoku Iji Kikaku no Gaiyo, Japan Society of Maintenology, Maintenology, Vol. 4, No. 3, p. 11-16, (2005) (in Japanese)
- [13] ISO 8686-1: Cranes-Design principles for loads and load combinations: Part1 General (1989).
- [14] ISO 8686-2: Cranes-Design principles for loads and load combinations: Part2 Mobile cranes (2004).
- [15] ISO 2394: General principles on reliability for structures, Third edition (1998).
- [16] JIS B 9955: 2017, General principles on reliability for mechanical products
- [17] Sakai, S.: Aratana Genshiryoku Gainen no Kouchiku wo Mezashite, ASME workshop report, Journal of the Society of Mechanical Engineers, Vol. 116, No. 1131, p. 123, (2013) (in Japanese)
- [18] https://www.jsme.or.jp/shinsai3.11/ASME%20Presidential%20Report%20full_032.pdf
- [19] Sakai, S.: Probabilistic method to determine allowable stress, Journal of High Pressure Institute of Japan, Vol. 60, Issue 1, p. 18-23, (2022)
- [20] ISO 11119-3: Gas cylinders-refillable composite gas cylinders and tubes. Part 3: fully wrapped fibre reinforced composite gas cylinders and tubes up to 450L with non-load-sharing metallic or nonmetallic liners. ISO, Geneva, CH(2013).

■ Author ■

Shinsuke Sakai