

行政院原子能委員會
委託研究計畫研究報告

功能安全應用研究
A Research of Functional Safety Application

計畫編號：1022001INER008

受委託機關(構)：中原大學

計畫主持人：劉益宏

聯絡電話：03-265-4301

E-mail address：lyh@cycu.edu.tw

核研所聯絡人員：陳昌國

報告日期：102 年 11 月 29 日

目 錄

目 錄	i
中文摘要	ii
Abstract.....	iii
壹、計畫緣起與目的	1
一、可靠性參數最佳化 (RELIABILITY-BASED PARAMETER OPTIMIZATION; RBPO)	2
(一)改良型可靠度指標法 (Modified Reliability Index Approach; MRIA)	3
(二)表現量測法 (Performance Measure Approach; PMA)	4
貳、研究方法與過程	6
一、表現量測法的不穩定性	6
二、混合可靠度法 (HYBRID RELIABILITY APPROACH; HRA)	7
參、主要發現與結論	11
一、非線性數學問題的驗證	11
二、結論與討論	16
肆、成果發表	17
一、論文投稿審核中 (一)	17
二、論文投稿審核中 (二)	17
伍、參考文獻	18

中文摘要

功能安全應用在多個工業領域是一項重要的研究，系統安全的函數功能包含了建立模型、數值分析、參數最佳化及可靠度評估等。可靠性參數最佳化有兩個傳統方法：改良型可靠度指標法(MRIA)與表現量測法(PMA)，國內外學術與業界皆廣泛使用兩方法來尋找滿足系統可靠度範圍的最佳設計參數。可靠度指標法在最佳化的過程中能穩定地找到最佳參數，而表現量測法具有較高的計算效率。本研究研發了混合可靠度法(HRA)，整合兩個傳統方法的優點於一身。透過可靠度分析的基本公式及兩傳統方法在最佳化過程中的特性，本研究推導出一個選擇因子，在最佳化過程中挑選最適合的演算法進行可靠度分析。幾個非線性數學問題的結果說明了混合可靠度法能夠穩定且高效地找到最佳可靠性參數，本研究方法將適用於各種功能安全應用。

Abstract

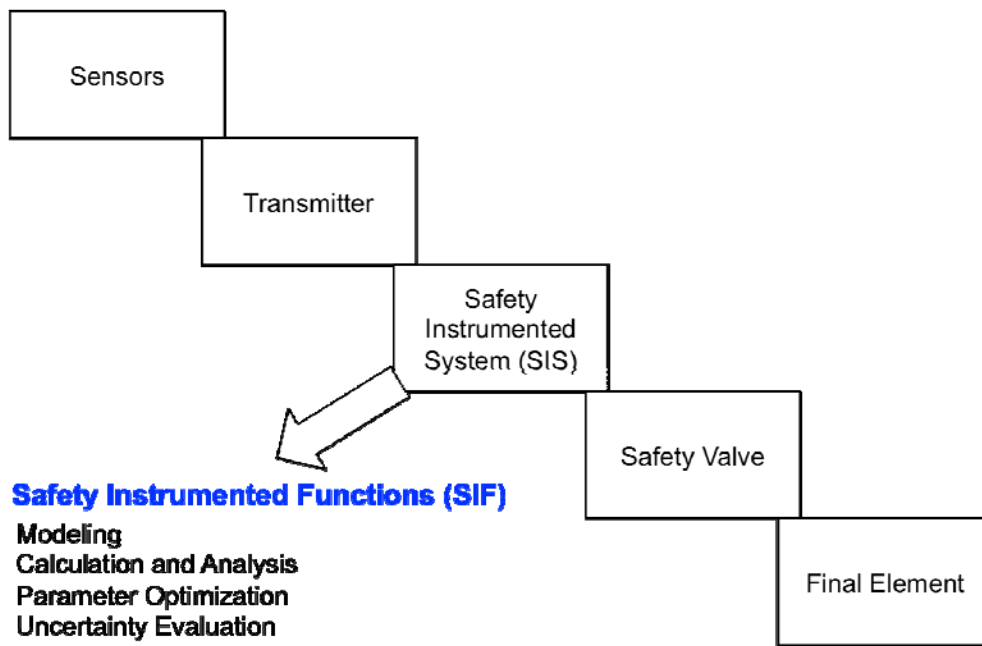
Two Reliability-Based Parameter Optimization (RBPO) methods, Modified Reliability Index Approach (MRIA) and Performance Measure Approach (PMA), have been widely utilized to find the optimal parameter settings in various applications under uncertainty. MRIA can stably find the optimal solutions during the optimization processes; however, PMA requires fewer computational calculations than MRIA. A selection factor has been derived based on the optimality conditions of both algorithms and a Hybrid Reliability Approach (HRA) has been developed to merge their advantages together. Some numerical examples have been used to compare the performances of the proposed and the existing methods. It is expected that the HRA can be embedded to any functional safety applications to improve the system reliability and to maintain acceptable stability.

壹、計畫緣起與目的

工程應用的驗證與核對過程(Data Validation and Reconciliation; DVR)中,使用資訊與數學方法自動化量測與修正功能應用的重要函數與參數,DVR 從原始量測數據中擷取準確及可靠的有用資訊,用來建立具有高度穩定性的資訊集合以代表實際應用運作的過程。

工業生產過程(如化學、化工、煉油、石油、天然氣等生產工廠,或是發電廠的熱力學過程)具有下列兩重要要素:(一)反映過程總體結構的數學模型、(二)反映任意時間的過程狀態的資料與數據。數學模型可以包含許多不同層次的資訊,例如:能量平衡的物理現象、質能之間的轉換定則,任何物理現象皆能以數學函數的方式表示。工程應用的重要參數為系統設計的控制變量,關鍵目標指標為系統的設計目標函數,而其他符合物理原則、經濟效益等的規則指標則為系統設計的限制函數。

功能安全應用在多個工業領域皆是一項重要的研究,系統安全的函數功能包含了建立模型、數值分析、參數最佳化及可靠度評估等,其中可靠度的評估攸關於系統應用的安全性。在各類工業應用中,設計不確定性的存在是無可避免的。傳統的設計最佳化演算法在限制條件範圍中改變設計變量,試圖找到可行範圍中的最佳設計目標。然而傳統最佳化演算法並未考慮設計不確定性,因此系統的失效機率可能高至百分之五十以上。



圖一、感測器、終端元素、安全儀表系統、安全儀表函數及可靠性最佳參數控制之間的關係

一、可靠性參數最佳化 (Reliability-Based Parameter Optimization; RBPO)

傳統可靠性參數最佳化有兩個傳統方法：改良型可靠度指標法 (MRIA) [1-3] 與表現量測法(PMA) [4]，國內外學術與業界皆廣泛使用兩方法來尋找滿足系統可靠度範圍的最佳設計參數[5-7]。可靠性最佳化設計的基本設計公式為：

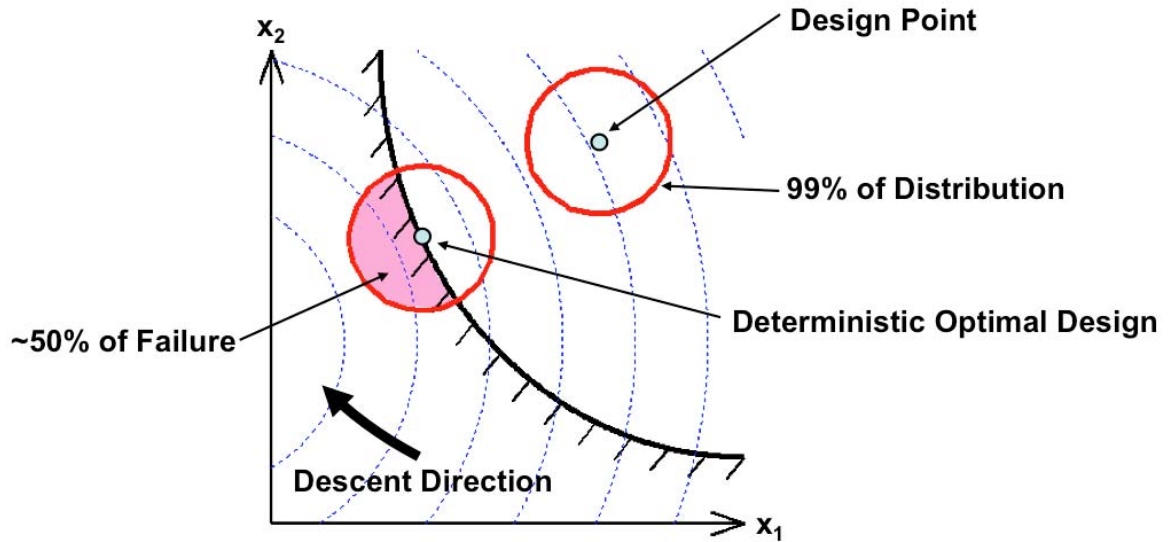
$$\begin{aligned} & \text{Min}_d \quad y(d) \\ & \text{s.t.} \quad P[g_i(\mathbf{X}) > 0] \leq P_{f,i} \quad i = 1 \square n \end{aligned}$$

上述公式中的機率計算需要大量的函數分析次數：

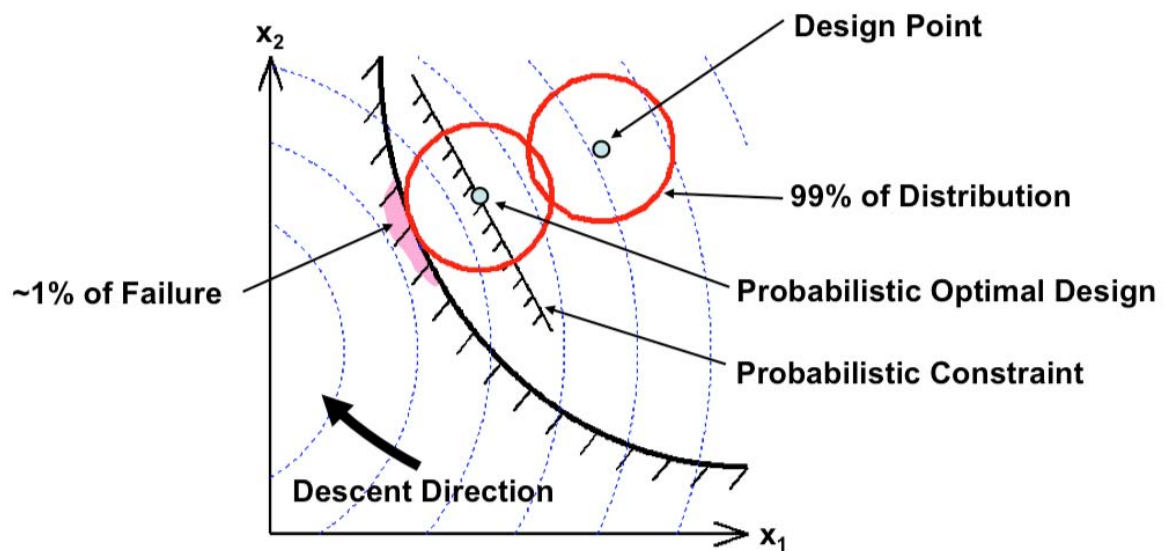
$$P[g(\mathbf{X}) > 0] = \int_{g>0} f(\mathbf{x}) d\mathbf{x}$$

雖然能夠準確地評估限制條件失效機率，但是計算效率過低[8-12]，因

此需要更效率的近似可靠度分析演算法。



(a)



(b)

圖二、可靠性參數最佳化基本知識：(a)未使用可靠性分析時失效率過高、(b)目標推導可靠性限制條件即能控制失效率

(一)改良型可靠度指標法 (Modified Reliability Index Approach;

MRIA)

可靠度指標法先計算設計點在標準常態設計空間(Standard Normal Space)中其至限制條件的距離，即安全係數的概念。該設計距離稱作可靠度指標(Reliability Index)，計算方式為

$$\beta_i = \frac{\mathbf{u}_i^* \cdot \nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|}$$

其中 \mathbf{u}_i^* 叫做最可能失效點，即標準常態分布空間中在限制條件邊界上離設計變量最近的設計點。根據可靠度指標值的計算，失效機率的計算為

$$P[g_i(\mathbf{X}) > 0] \cong \Phi(-\beta_i)$$

其中 Φ 為累積分布機率計算函數(Cumulative Distribution Function)。將原始設計最佳化問題轉換至機率指標空間，即使用反累積分布運算 Φ^{-1} ，原始設計問題變成：

$$\begin{aligned} \text{Min}_{\mathbf{d}} \quad & y(\mathbf{d}) \\ \text{s.t.} \quad & -\beta_i(\mathbf{d}) \leq -\beta_{f,i} \quad i=1\dots n \end{aligned}$$

$\beta_{f,i}$ 即為容許可靠度指標。將可靠度指標代入並執行線性展開，該機率性限制函數近似為下列函數：

$$\frac{\mathbf{u}_i^* \cdot \nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|} - (\mathbf{d} - \mathbf{d}^{(k)}) \cdot \frac{\nabla_{\mathbf{d}} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|} \leq \beta_{f,i}$$

可靠度指標法的計算需要較高的運算量，但是具有高度的穩定性及準確性。

(二)表現量測法 (Performance Measure Approach; PMA)

反之，表現量測法[5-7, 13]採用較高效率的運算，來找尋設計變量

周圍容許可靠度半徑上的最可能失效目標點 $\mathbf{u}_i^\#$ ，並評估設計的可能最差表現值，只要可能最差表現值滿足容許範圍，此設計具有足夠的可靠性。表現量測值的評估方式[4]如下：

$$\gamma_i(\mathbf{d}) = F_{g_i}^{-1} \left\{ 1 - \Phi \left[-\beta_{f,i} \right] \right\}$$

F_{g_i} 是限制條件函數值低於 γ 的機率。根據表現量測的分析方式，原始設計最佳化問題轉型為：

$$\begin{aligned} \underset{\mathbf{d}}{\text{Min}} \quad & y(\mathbf{d}) \\ \text{s.t.} \quad & \gamma_i(\mathbf{d}) \leq 0 \quad i=1 \dots n \end{aligned}$$

將最可能失效目標點代入並線性展開，因此得到近似機率性限制函數：

$$g_i(\mathbf{u}_i^\#) + (\mathbf{d} - \mathbf{d}^{(k)}) \cdot \nabla_{\mathbf{d}} g_i(\mathbf{u}_i^\#) \leq 0$$

貳、研究方法與過程

一、表現量測法的不穩定性

表現量測法的反可靠度分析中，無法永遠保證最可能機率設計點落在極限邊界 $g_i(\mathbf{u}_i)=0$ 上，因此有可能在不可行區域(Infeasible Space) 找到設計點，然後不可行區域中的分析在許多狀況下是無法取得的，強制計算或評估的後果是系統無法承擔的或不可容許的。表現量測法雖然具有較高效率的最可能機率設計點迭代過程[14]，其不穩定性卻是系統分析中的不安定因子，必須研發新的演算法將其不安定的問題解決。

在可靠度參數設計中，能夠避免不適當的可靠度分析是很重要的，因為不適當的分析可能遭致最佳化過程的不穩定或是迭代過程的效率降低。Youn 等人[15]曾使用決定性最佳化設計點作為可靠性最佳化設計過程的初始點，然而仍然不能確保最可能失敗目標點落在可行域當中。因此本計劃研究的一項重要目標就是解決表現量測法不穩定的問題，第二目標是如何承襲表現量測法的高效率迭代過程，第三目標則是希望利用可靠度指標法的穩定迭代過程來彌補表現量測法的不足。

二、混合可靠度法 (Hybrid Reliability Approach; HRA)

本研究研發了混合可靠度法(HRA)，整合兩個傳統方法的優點於一身。透過可靠度分析的基本公式及兩傳統方法在最佳化過程中的特性，本研究推導出一個選擇因子，在最佳化過程中挑選最適合的演算法進行可靠度分析。當設計變量接近最佳解時，MRIA 與 PMA 的近似限制條件收斂於同一限制函數，故下列兩方程式相等：

$$-\frac{\mathbf{u}_i^* \cdot \nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|} + \beta_{f,i} + (\mathbf{d} - \mathbf{d}^{(k)}) \cdot \frac{\nabla_{\mathbf{d}} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|} = 0$$

$$\frac{g_i(\mathbf{u}_i^\#)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^\#)\|} + (\mathbf{d} - \mathbf{d}^{(k)}) \cdot \frac{\nabla_{\mathbf{d}} g_i(\mathbf{u}_i^\#)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^\#)\|} = 0$$

另外，因為 $\nabla_{\mathbf{d}} g_i(\mathbf{u}_i^*) \cong \nabla_{\mathbf{d}} g_i(\mathbf{u}_i^\#)$ ，推導出下列方程式：

$$\frac{g_i(\mathbf{u}_i^\#)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^\#)\|} + \frac{\mathbf{u}_i^* \cdot \nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)}{\|\nabla_{\mathbf{u}_i} g_i(\mathbf{u}_i^*)\|} - \beta_{f,i} = 0$$

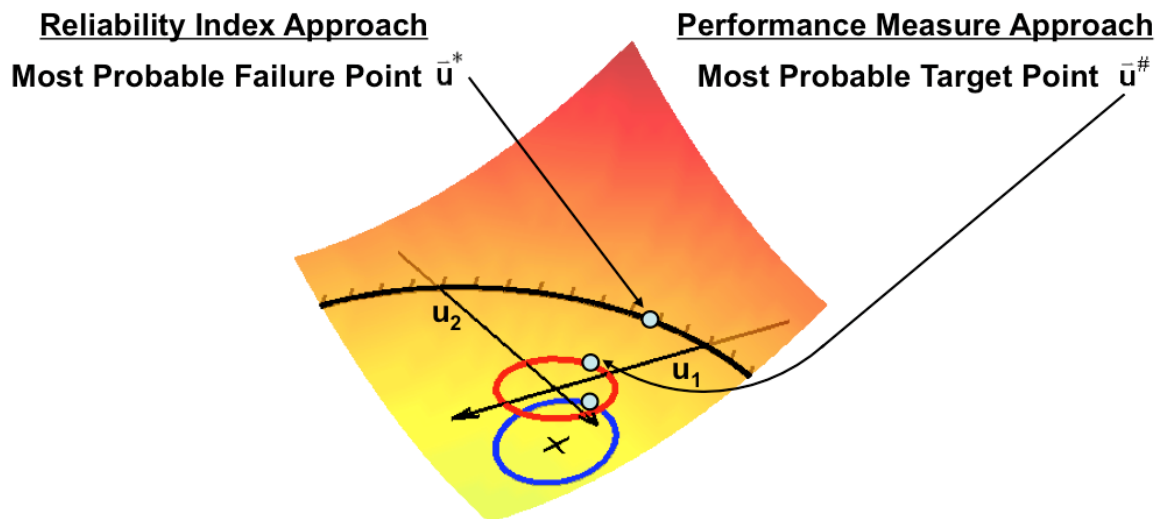
依設計變量進行函數與梯度近似，定義下列選擇因子：

$$S_i \equiv \frac{g_i(0)}{\|\nabla_{\mathbf{u}_i} g_i(0)\|} + \beta_{f,i}$$

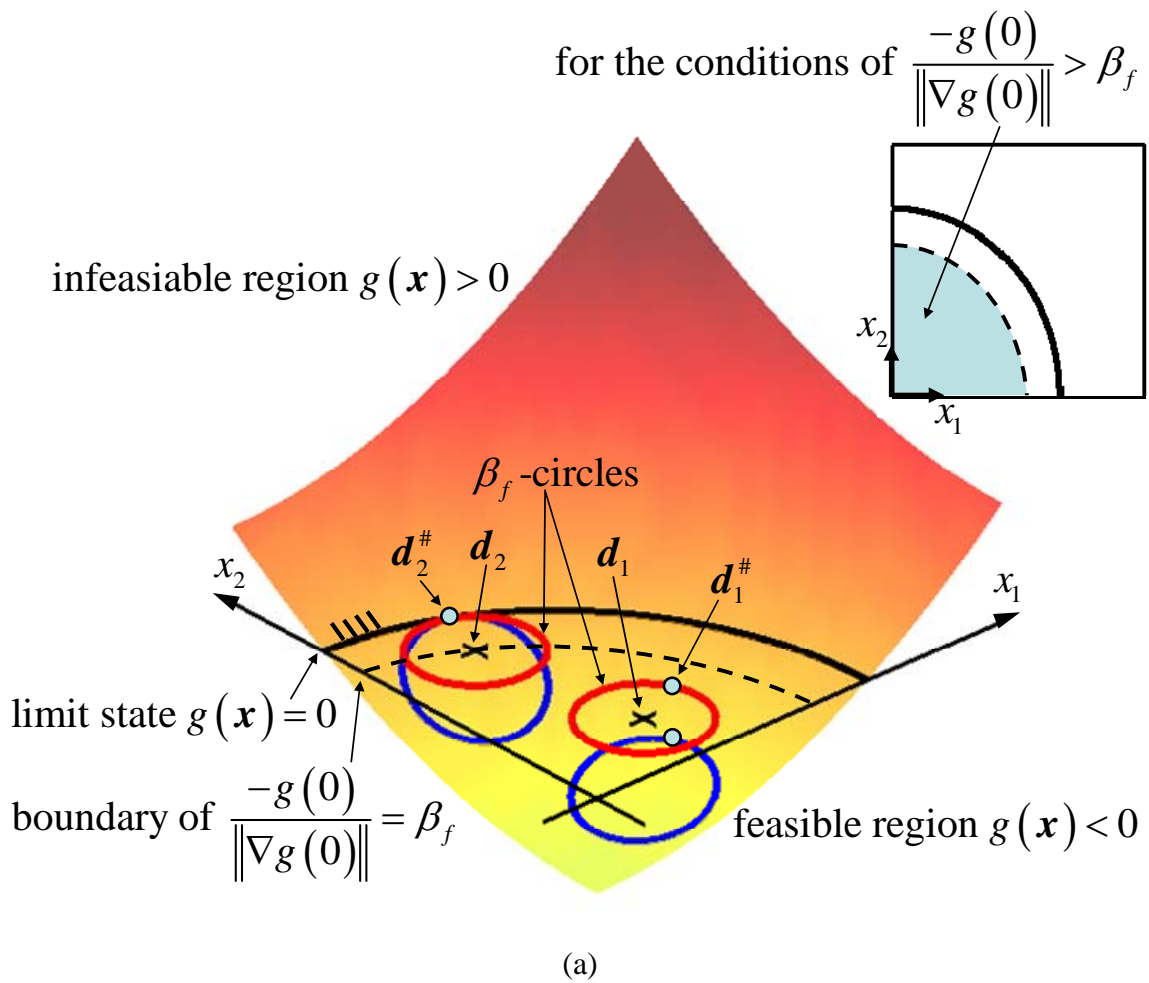
當 S_i 接近零時，MRIA 與 PMA 的近似機率性函數幾乎達到收斂，故使用效率較高的 HRA；當選擇因子為負值，設計變量落在可行域，本演算法假設可行區域全為有限(finite)，因此建議使用效率高的 PMA；若選擇因子為正值，設計變量落在不可行域，限制函數可能為高度非線性或甚至無限(infinite)，故建議使用穩定性高的 MRIA，以確保能順利找到最可能失效點。圖三說明了兩個演算法的不同之處，圖四示範了所有可能發生的狀況，其中子圖(a)建議使用效率較高的 PMA，而在子圖(b)的狀況下建議使用穩定性高的 MRIA，因此本研究研發的

HRA 能夠兼具兩個演算的優點：高效且穩定。

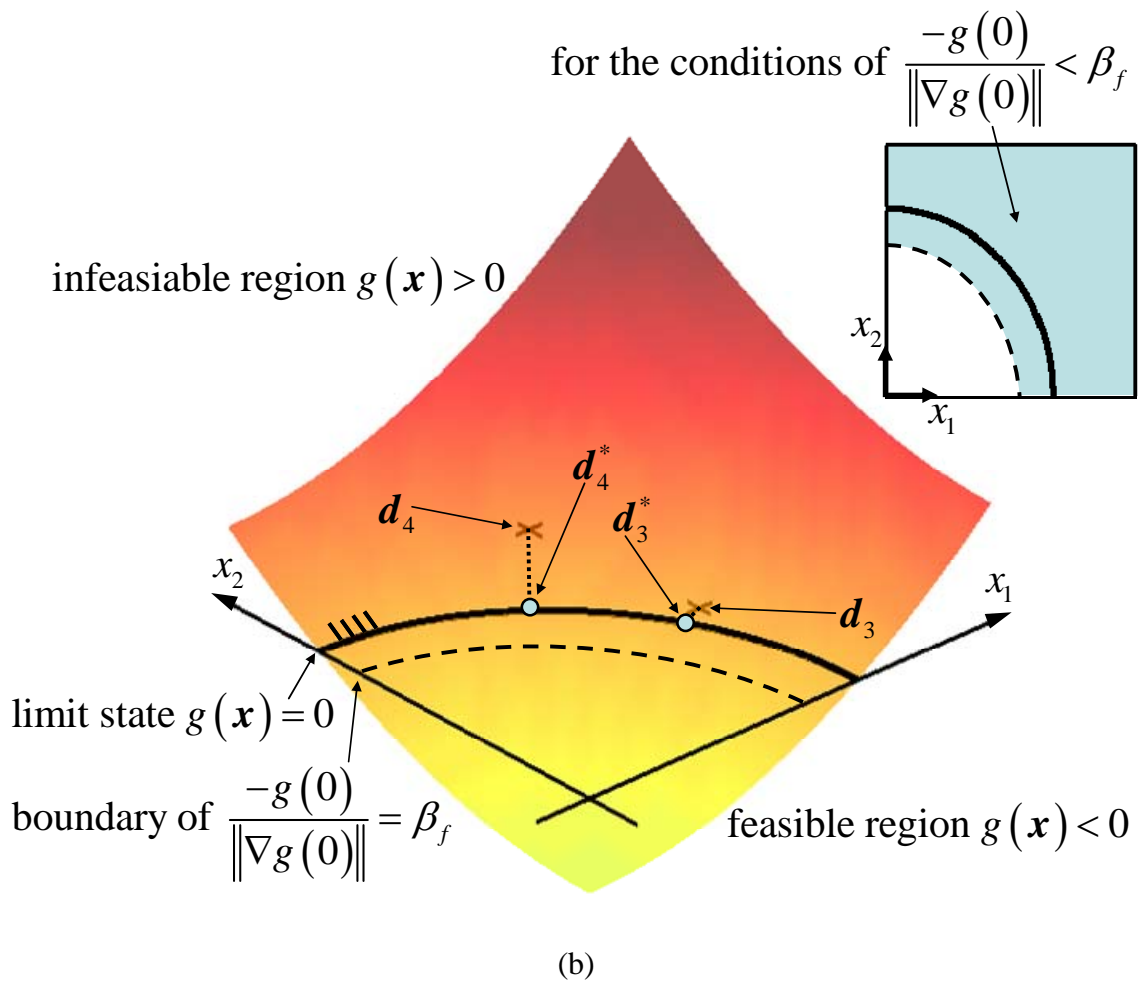
HRA 的迭代過程如下：在每次迭代的初始步驟，先評估每個限制條件的選擇因子 S_i ，若選擇因子為正值，使用穩定的 MRJA；反之，使用高效的 PMA。反覆此迭代步驟，直到收斂為止。HRA 使用的選擇因子計算不需要使用額外的函數運算，因為 $g_i(0)$ 及 $\nabla_{u_i} g(0)$ 在兩可靠度分析法中皆已計算。



圖三、RIA 與 PMA 尋找最可能失效點的不同之處



圖四、基於選擇因子挑選適當演算法執行可靠性最佳化：(a)選擇 PMA 的狀況、(b)選擇 MRJA 的狀況



圖四、基於選擇因子挑選適當演算法執行可靠性最佳化 (Continued) :

(a)選擇 PMA 的狀況、(b)選擇 MRJA 的狀況

參、主要發現與結論

本研究計畫研發的 HRA 為一個標準可靠性最佳化設計演算法，適用於各種功能安全應用函數中，且能延伸至其他不同最可能失效點分析法：進階均值分析法[9]、一階可靠度分析法[1, 2]、二階可靠度分析法[12]、混合均值分析法[14]、進階混合均值分析法[6]。另外，HRA 也能用來延伸至其他可靠性最佳化設計演算法：限制函數平移法[16-18]、變量平移法[19]。HRA 亦能用於非常態分析數學模型[20]上。

一、非線性數學問題的驗證

本研究使用了幾個非線性數學問題[3, 17, 18, 20-25]驗證混合可靠度法的效能。算例一的題目為：

$$\begin{aligned} \text{Min}_d \quad & y(\mathbf{d}) = d_1 + d_2 \\ \text{s.t.} \quad & P_i[g_i(\mathbf{X}) > 0] \leq P_f \quad i=1\dots3 \\ & 0 \leq d_j \leq 10 \quad j=1,2 \end{aligned}$$

其中

$$\begin{aligned} g_1(\mathbf{X}) &= 1 - \frac{X_1^2 X_2}{20} \\ g_2(\mathbf{X}) &= 1 - \frac{(X_1 + X_2 - 5)^2}{30} - \frac{(X_1 - X_2 - 12)^2}{120} \\ g_3(\mathbf{X}) &= 1 - \frac{80}{X_1^2 + 8X_2 + 5} \end{aligned}$$

容許失效機率定義為 0.13%，即三標準差設計。隨機設計變量的標準差分別為 $[\sigma_1, \sigma_2] = [0.3, 0.3]$ 。子迭代過程的最大迭代次數為五，最佳化迭代過程的終止條件為目標函數的誤差低於 10^{-3} 。

第二算例的題目為：

$$\begin{aligned} \underset{\mathbf{d}}{\text{Min}} \quad & y(\mathbf{d}) \\ \text{s.t.} \quad & P_i[g_i(\mathbf{X}) > 0] \leq 5\% \quad i=1\dots 3 \\ & d_1 \in [2, 7], d_2 \in [0.5, 5.5] \\ & [\sigma_1, \sigma_2] = [0.5, 0.5] \end{aligned}$$

其中

$$y(\mathbf{d}) = -\frac{(d_1 + d_2 - 10)^2}{30} - \frac{(d_1 - d_2 + 10)^2}{120}$$

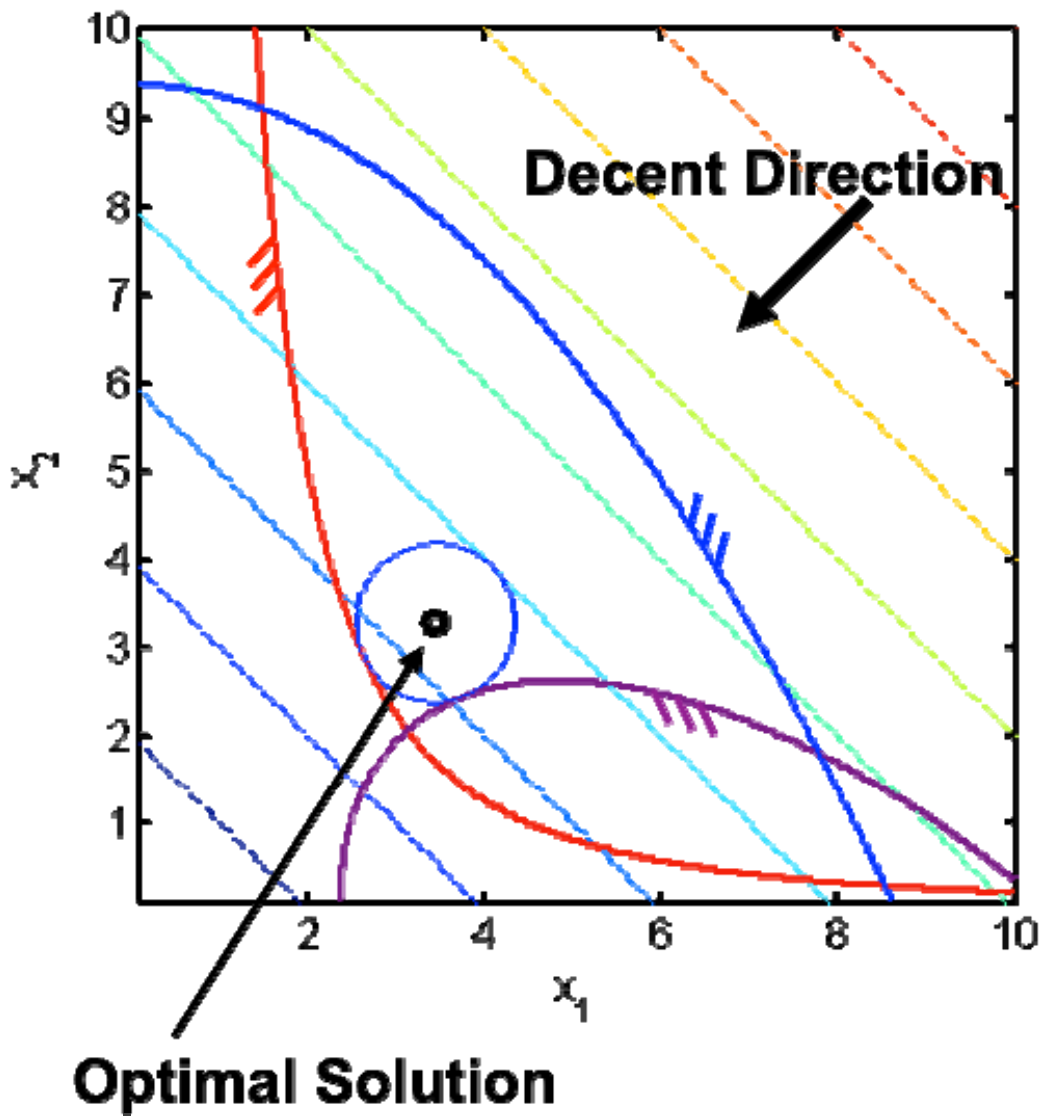
$$g_1(\mathbf{X}) = 1 - \frac{X_1^2 X_2}{20}$$

$$\begin{aligned} g_2(\mathbf{X}) = & -1 + (0.9063X_1 + 0.4226X_2 - 6)^2 + (0.9063X_1 + 0.4226X_2 - 6)^3 \\ & - 0.6(0.9063X_1 + 0.4226X_2 - 6)^4 - (-0.4226X_1 + 0.9063X_2) \end{aligned}$$

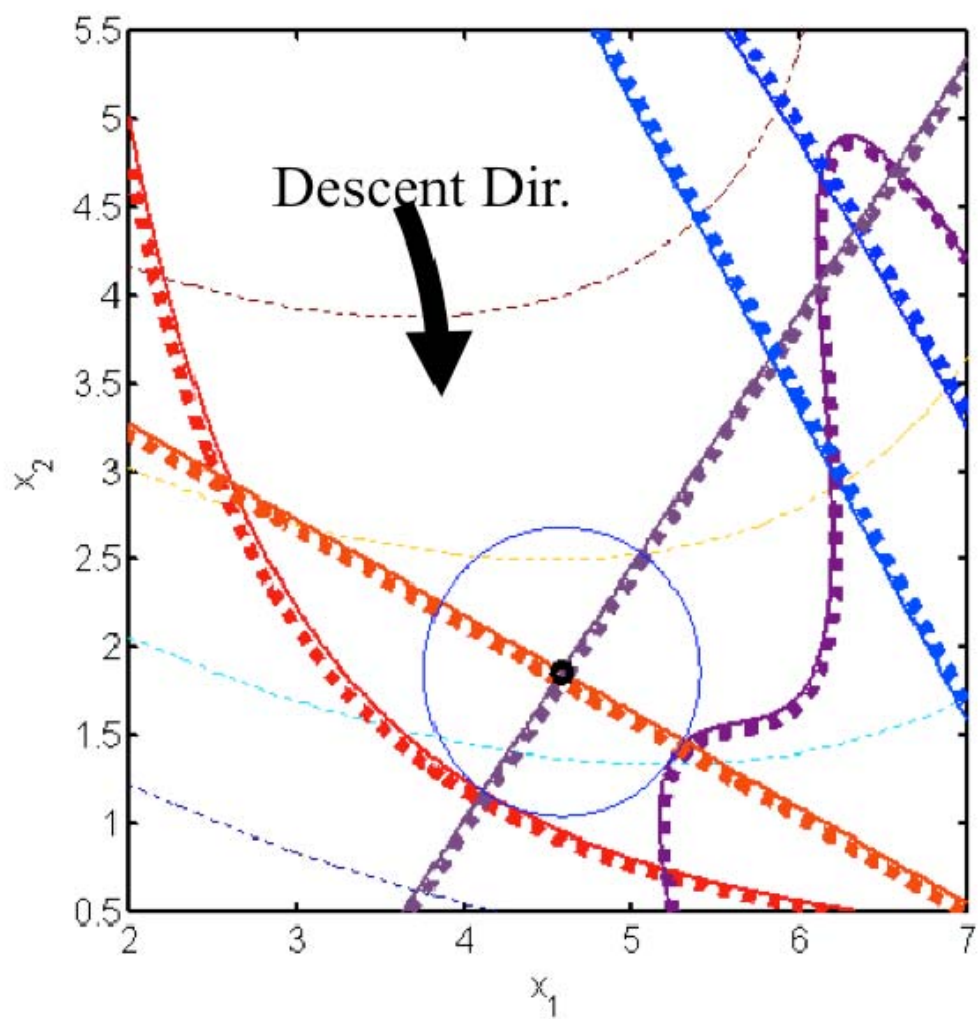
$$g_3(\mathbf{X}) = 1 - \frac{80}{X_1^2 + 8X_2 + 5}$$

其他最佳化設計如同算例一。

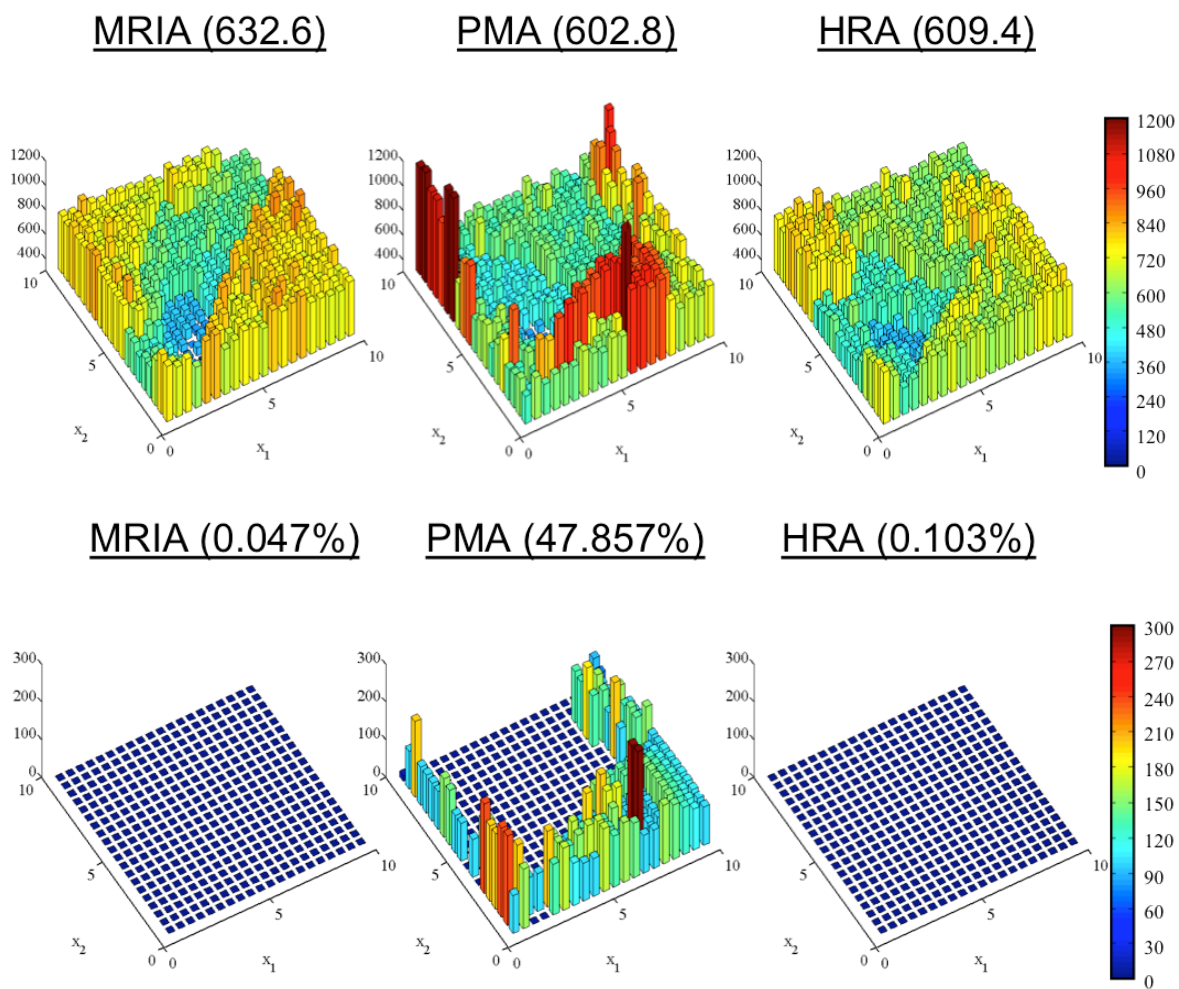
在設計空間中採用了 400 個設計初始點，分別使用 MRJA、PMA 及 PMA 三個方法來解決算例一與算例二兩個問題，圖五與圖六顯示了數學算例一與二的最佳參數設計點，圖七與圖八顯示了兩個算例的結果。我們發現 MRJA 一般而言使用較高的電腦計算量(Function Count; FC)，但具有高度的穩定性，因為限制條件違背累積量(Sum of Violation; SOV)極低；PMA 效率較高，使用較低的電腦計算量，但是其有時候無法正常收斂；因此本研究採用 HRA，其效率等如 PMA 般高，且其穩定性如同 MRJA 一般。此結果說明了混合可靠度法能夠穩定且高效地找到最佳可靠性參數，本研究方法將適用於各種功能安全應用。



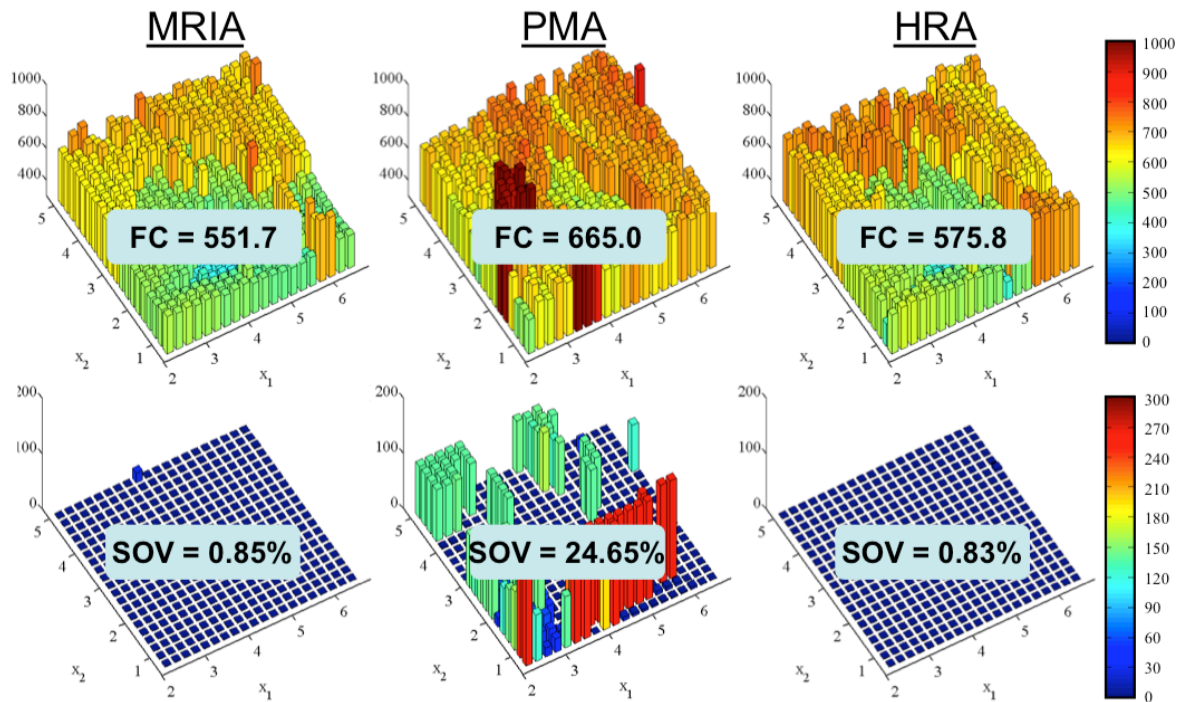
圖五、數學算例一的可靠性最佳參數設計點



圖六、數學算例二的可靠性最佳參數設計點



圖七、數學算例一的結果



圖八、數學算例二的結果

二、結論與討論

本研究計畫除了回顧了兩個傳統的可靠度參數最佳化演算法：可靠度指標法與表現量測法，研發了混合可靠度法，囊括了兩個傳統演算法的優點：可靠度指標法的高穩定性及表現量測法的高計算效率。混合可靠度法的計算方式雖包含了額外的選擇因子計算，但是並不需要額外的函數運算量。由兩個非線性數學算例的驗證中，我們發現混合可靠度法不但具備了可靠度指標法的高度穩定性，且效率可以媲美表現量測法。

肆、成果發表

一、論文投稿審核中（一）

Yi-Hung Liu, Yung Ting, Shian-Shing Shyu, Chang-Kuo Chen, Mu-Der Jeng

“A Support Vector Data Description Committee for Face Detection”

Mathematical Problem in Engineering, 2013

(Accept with minor revision) (SCI)

二、論文投稿審核中（二）

Po Ting Lin, Mark Christian E. Manuel, Yi-Hung Liu, Yu-Cheng Chou, Yung Ting, Shian-Shing Shyu, Chang-Kuo Chen, Chun-Lin Lee

“A Multifaced Approach for Safety and Reliability-Based Design Optimization”

Quality Engineering, 2013

(Under review) (SCI)

伍、參考文獻

- [1] A. M. Hasofer and N. C. Lind, "Exact and Invariant Second-Moment Code Format," *Journal of the Engineering Mechanics Division*, vol. 100, no. EM1, pp. 111-121, 1974.
- [2] R. Rackwitz and B. Fiessler, "Structural Reliability under Combined Random Load Sequences," *Computers & Structures*, vol. 9, pp. 489-494, 1978.
- [3] P. T. Lin, H. C. Gea, and Y. Jaluria, "A Modified Reliability Index Approach for Reliability-Based Design Optimization," *Journal of Mechanical Design*, vol. 133, no. 4, 044501, 2011.
- [4] J. Tu, K. K. Choi, and Y. H. Park, "A New Study on Reliability Based Design Optimization," *Journal of Mechanical Design*, vol. 121, pp. 557-564, 1999.
- [5] K. Maute and D. M. Frangopol, "Reliability-Based Design of Memes Mechanisms by Topology Optimization," *Computers & Structures*, vol. 81, pp. 813-824, 2003.
- [6] B. D. Youn, K. K. Choi, and L. Du, "Adaptive Probability Analysis Using an Enhanced Hybrid Mean Value Method," *Structural and Multidisciplinary Optimization*, vol. 29, no. 2, pp. 134-148, 2005.
- [7] L. Du and K. K. Choi, "An Inverse Analysis Method for Design Optimization with Both Statistical and Fuzzy Uncertainties," *Structural and Multidisciplinary Optimization*, vol. 37, no. 2, pp. 107-119, 2008.
- [8] B. M. Ayyub and A. Haldar, "Practical Structural Reliability Techniques," *Journal of Structural Engineering*, vol. 110, no. 8, pp. 1707-1724, 1984.
- [9] Y. T. Wu, O. H. Burnside, and T. A. Cruse, "Probabilistic Methods for Structural Response Analysis," *Computational Mechanics of Probabilistic and Reliability Analysis*, W. K. Lam and T. Belytschko, Eds., pp. 181-196, Elme Press International, Lausanne, Switzerland, 1989.

- [10] L. P. Wang and R. V. Grandhi, "Efficient Safety Index Calculation for Structural Reliability Analysis," *Computers & Structures*, vol. 52, no. 1, pp. 103-111, 1994.
- [11] L. P. Wang and R. V. Grandhi, "Intervening Variables and Constraint Approximations in Safety Index and Failure Probability Calculations," *Structural and Multidisciplinary Optimization*, vol. 10, no. 1, pp. 2-8, 1995.
- [12] H. O. Madsen, S. Krenk, and N. C. Lind, *Methods of Structural Safety*, Prentice-Hall, Englewood Cliffs, NJ, 1986.
- [13] R. Y. Rubinstein, *Simulation and the Monte Carlo Method*, Wiley, New York, NY, 1981.
- [14] B. D. Youn, K. K. Choi, and Y. H. Park, "Hybrid Analysis Method for Reliability-Based Design Optimization," *Journal of Mechanical Design*, vol. 125, pp. 221-232, 2003.
- [15] B. D. Youn, K. K. Choi, and L. Du, "Enriched Performance Measure Approach for Reliability-Based Design Optimization," *AIAA Journal*, vol. 43, no. 4, pp. 874-884, 2005.
- [16] Y. T. Wu, Y. Shin, R. Sues, and M. Cesare, "Safety-Factor Based Approach for Probability-Based Design Optimization," 42nd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference and Exhibit, Seattle, WA, 2001.
- [17] B. D. Youn and K. K. Choi, "Selecting Probabilistic Approaches for Reliability-Based Design Optimization," *AIAA Journal*, vol. 42, no. 1, pp. 124-131, 2004.
- [18] I. Lee, K. K. Choi, L. Du, and D. Gorsich, "Inverse Analysis Method Using Mpp-Based Dimension Reduction for Reliability-Based Design Optimization of Nonlinear and Multi-Dimensional Systems," *Computer Methods in Applied Mechanics and Engineering*, vol. 198, no. 1, pp. 14-27, 2008.
- [19] X. Du and W. Chen, "Sequential Optimization and Reliability

- Assessment Method for Efficient Probabilistic Design," *Journal of Mechanical Design*, vol. 126, pp. 225-233, 2004.
- [20] B. D. Youn and K. K. Choi, "An Investigation of Nonlinearity of Reliability-Based Design Optimization Approaches," *Journal of Mechanical Design*, vol. 126, no. 3, pp. 403-411, 2004.
- [21] R. J. Yang and L. Gu, "Experience with Approximate Reliability-Based Optimization Methods," *Structural and Multidisciplinary Optimization*, vol. 26, no. 2, pp. 152-159, 2004.
- [22] G. Cheng, L. Xu, and L. Jiang, "A Sequential Approximate Programming Strategy for Reliability-Based Structural Optimization," *Computers & Structures*, vol. 84, no. 21, pp. 1353-1367, 2006.
- [23] P. Yi, G. Cheng, and L. Jiang, "A Sequential Approximate Programming Strategy for Performance-Measure-Based Probabilistic Structural Design Optimization," *Structural Safety*, vol. 30, no. 2, pp. 91-109, 2008.
- [24] P. Yi and G. Cheng, "Further Study on Efficiency of Sequential Approximate Programming for Probabilistic Structural Design Optimization," *Structural and Multidisciplinary Optimization*, vol. 35, no. 6, pp. 509-522, 2008.
- [25] H. C. Gea and K. Oza, "Two-Level Approximation Method for Reliability-Based Design Optimisation," *International Journal of Materials and Product Technology*, vol. 25, no. 1/2/3, pp. 99-111, 2006.