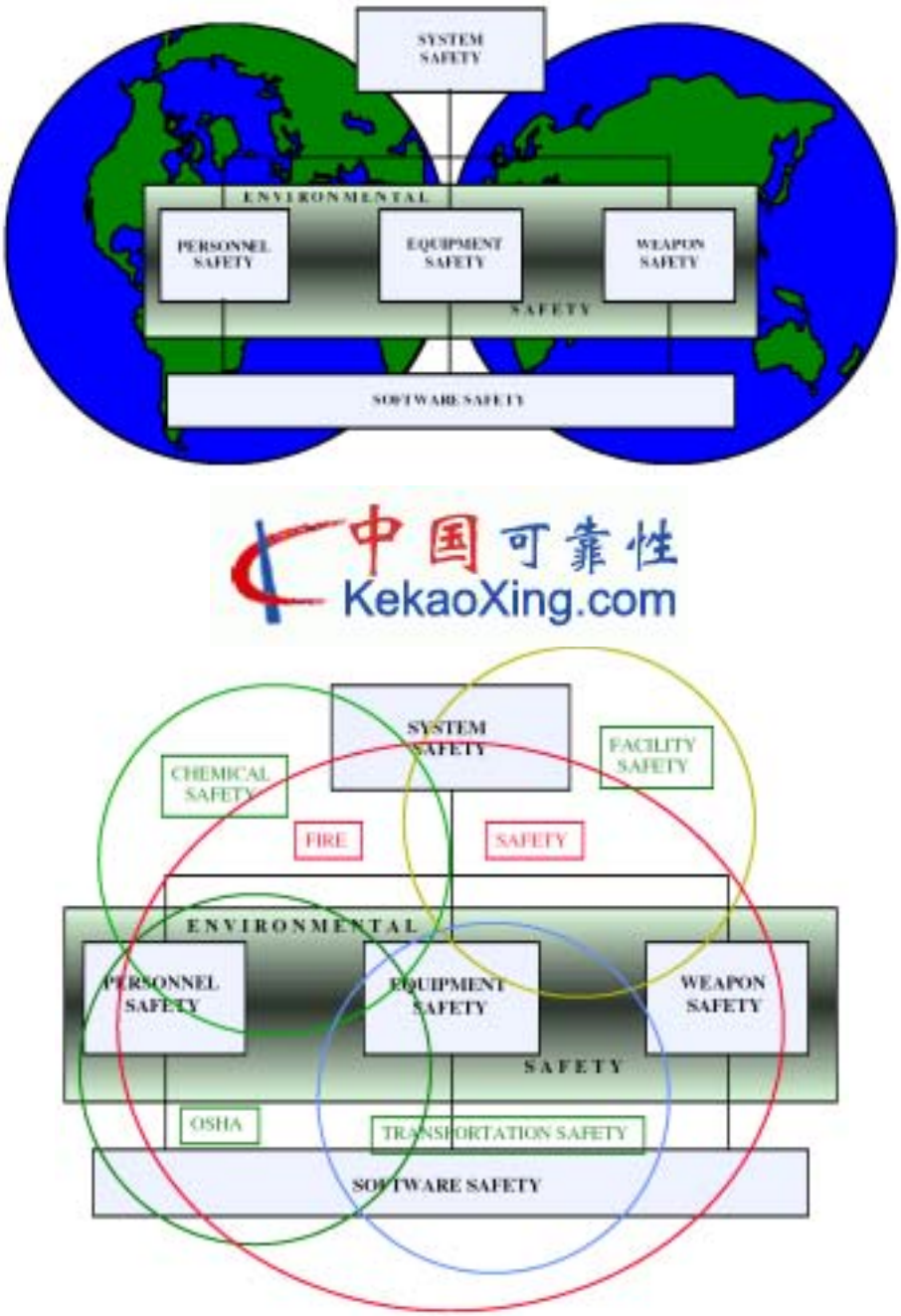
1 前言



中国可靠性
KekaoXing.com

圖 2：系統安全技術領域

中国可靠性网 http://www.kekaoxing.com

2 系統安全

2.1 系統安全緣起

系統安全(System Safety)的概念是 1963 年美國空軍司令部正式提出的軍用標準 MIL-S-38130, 系統與相關次系統、設備之系統安全工程一般需求(System Safety Engineering of Systems and Associated Subsystems and Equipment, General Requirement for)。1967 修定為 A 版，亦即 MIL-S-38130A，成為各軍種、大公司、大企業進行系統安全評價與訂定安全計畫方案的指導文件，美國航空暨太空總署(NASA)也把系統安全作為太空發展計畫中的一個基本項目。1969 年 7 月美國國防部發表了 MIL-STD-882：系統安全計畫需求(System Safety Program Requirements)，成為軍備合約的引用標準之一，並為許多大企業應用。1977 年 6 月修定為 A 版、1984 年 3 月修定為 B 版、1993 年 1 月修訂為 C 版，最新版本則為 2000 年 2 月發佈的 D 版。主要的程序是從系統安全分析、危害性評價、比較綜合評價、最佳化計畫決策，再反饋到系統安全分析，最後得到符合需求的系統安全。

目前，系統安全以從創始期進入應用期，近年來，由於如美國三里島核電廠事件、前蘇聯車諾比核電廠事件、印度博帕爾聯合碳化公司毒氣洩漏事件等重大事件相繼發生，使世界各國關注系統安全性與可靠度問題，國際勞工組織(International Labour Organization, ILO)在 1986 年 6 月第 71 屆大會通過一項決議：規定要採取措施來預防由於危險品和工業過程中的不安全而引起的危害與事故。系統的安全性與可靠度問題都是與人的因素有關的，近年來的安全工程、可靠度工程、維護度工程等學門不僅把硬體的可靠度等問題作為主要研究對象，進一步提出以人為主要研究對象的人機安全工程新課題。

2.2 安全性概念

安全在希臘文中的意思就是「完整」，在梵語中的意思是「沒有受傷」或「完整」，在拉丁文中則又有「衛生」的意涵。

中国可靠性网 http://www.kekaoxing.com

安全是指一種狀態，即某一元件、某一次系統或系統保持完整的一種狀態，安全性是指上述狀態能夠維持的能力，在可靠度用語中，安全性的意義是指在設計時，為使產品失效不致引起人身與物質等重大損失而採取的預防措施。

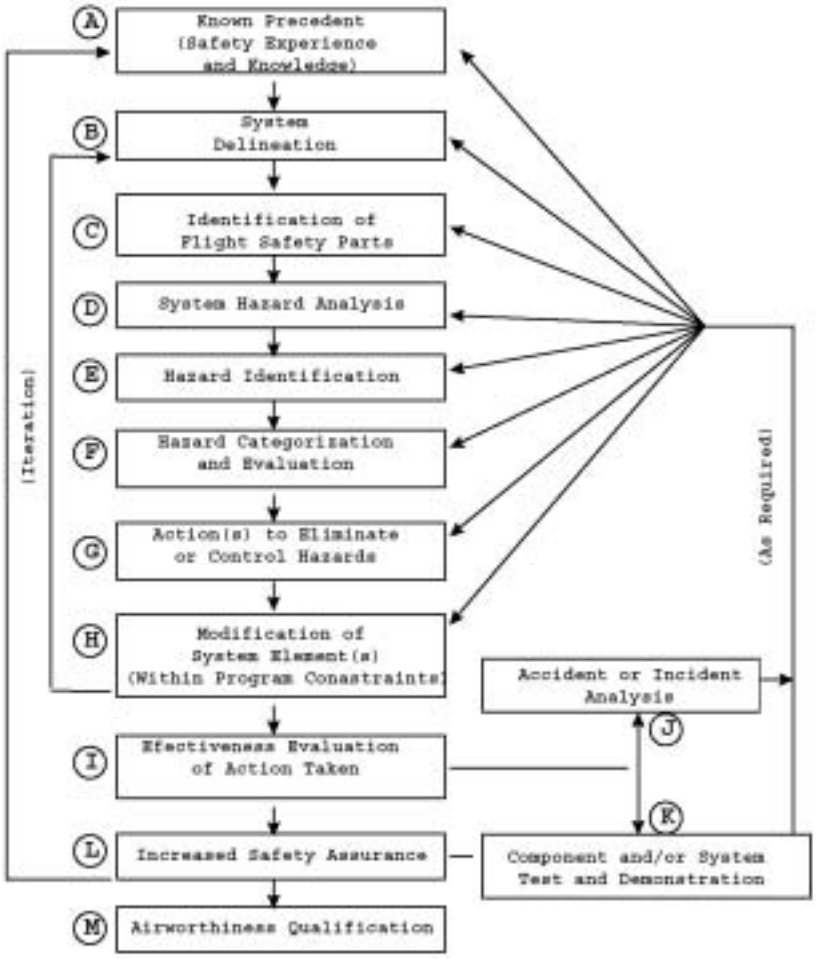


圖 1：系統安全過程

危害(Hazard)也是一種狀態，指某一元件、某一次系統或系統即將處於遭受破壞、不能保持完整的狀態，危害性是與安全性相對立的概念，即系統不能保持完整的一種特性。

沒有絕對安全，即安全狀態之中總是潛伏著一定的危害因素，所以研究安全性，就是研究如何減少危害性。

事故是指以下三種情況之一或其組合：

(1). 安全狀態遭到破壞時的某一個或若干事件的發生；

(2). 危害狀態的發展使某一個或事件發生，導致系統、次系統、或元件遭受破壞；

(3). 上述事件發生雖然未引起破壞，也足以使系統的操作發生永久性中斷或目標無法達成結果。

中国可靠性网 http://www.kekaoxing.com

2.3 元件安全與安全工程

元件安全(Component Safety)是安全工程(Safety Engineering)的重點研究課題之一，配合構成系統的各種元件的需要而延伸及發展出來的特殊專業技術，如化工安全、電氣安全、熱工安全、材料安全等，主要的研究目標是尋求有關元件不超過破壞的界限或某種臨界值。而元件的安全界限究竟對所構成的系統的安全性會發生什麼影響，不一定能夠在安全工程學中研究清楚，因此單獨、孤立的進行元件安全研究，只能說是局部的安全工程學。

系統安全是考慮元件之間的相戶關係、元件與人員之間的相戶關係、以及通過一整套分析、評價、運算等手段，考慮系統及其次系統不受到破壞的研究課題，它不僅與上述安全工程學的專業技術有關，而且可靠度工程、後勤工程、工業工程等亦有密切的關聯。

2.4 系統安全性

系統安全性是針對由人、機、環境的特定系統，在人的有效活動範圍與活動時間內，考慮成本、系統效率、環境條件、輸出的產量與品質等限制條件時，系統或其相關次系統、元件、人員能夠維持其免遭破壞或傷害的能力大小。系統安全性實際上就是其安全效能。

有人把系統安全性定義為「系統的最佳安全狀態」是不確切的，因為其一是用「安全狀態」定義「安全性」，在邏輯上不夠嚴謹，其二是用「最佳」的說法不確切，所謂最佳是在不考慮限制條件的簡單定義下的結論，這在理論上是容易的，但在實施系統安全的管理作法時卻不可能忽略，在技術上是否可行、在經濟上是否合理等問題。所以系統安全性只有「高低」的說法，而沒有「絕對安全」、「最佳安全」的說法。系統安全性高，是指該系統、次系統、元件或人員維持其不受破壞的狀態的能力大，反之則稱為安全性低。

2.5 系統安全性度量

安全性概念的反面是危害性，危害性可以作為衡量一個系統或次系統、元件、人員的安全性高低的定量指標。危害性大，則安全性低；危害性小，則安全性高。當危害性逐漸發展到無窮大就是系統受到破壞，人員發生傷亡，即系統發生災害或事故。

危害性的定量指標有下列幾種：

(1). 危害性等級

根據美軍標準 MIL-STD-882 提供的分級指標，危害性指標有下列四類等級：

A. 第 VI 類等級：Safe(安全的)

此一等級的危害性為 0；雖然系統或次系統、元件有失效(亦即可靠度不好)、或人員操作有錯誤，人、機、環境的聯結方式從設計上或人為上有缺陷，但沒有或不會造成系統或次系統的損壞、元件與設備的損壞、或人員的傷害。

B. 第 III 類等級：Marginal(臨界的)

中国可靠性网 http://www.kekaoxing.com

此一等級的危害性不為 0，但不很大，系統沒有受到破壞，但由於個別元件的損壞或人員能力的下降，造成系統的效能有所下降，系統可靠度較差，但系統的操作仍然能夠保持在正常的控制狀態下。

C. 第 II 等級：Critical(關鍵的)

此一等級的危害性極大，由於人員的失誤、元件的故障，或人、機、環境聯結方式在設計上的錯誤，使主要的次系統受到破壞，或已有人員傷亡、財物毀壞或滅失。此時，系統已不能處於正常控制狀態下可靠地操作，可靠度下降到零左右，雖然整個系統尚未受到損壞，但若不採取措施，將會向更惡化情況發展。

D. 第 I 類等級：Catastrophic(致命的)

此一等級的危害性已發展到無窮大，由於構成系統的人員或元件或次系統，以及其聯結方式的嚴重缺陷或事故，造成系統的破壞性損壞或人員的嚴重傷亡。

(2). 危害性係數

危害性等級也可以用「」

(3). 危害性要素

2.6 危害性分析

3 系統安全性管理

系統的安全效能管理，是以系統操作階段的安全性、可靠度為基礎的工程管理，包括發展、維持、改善系統的可靠度與維護度，為此要收集、分析數據與資訊，評價安全性程度，並及時採取措施，保證系統的正常操作。

安全性管理與安全管理不同，後者還包括勞工安全法規遵行、安全管理單位設置、安全技術規章的制訂，勞工安全衛生守則實施、防護器具的發放、安全衛生教育、作業安全管制、作業安全檢查等許多方面，有更為廣泛的內容。安全性管理只是

中国可靠性网 http://www.kekaoxing.com

安全管理中的一環，但卻是十分重要的一部分。系統安全性管理包括缺陷樹分析(Fault Tree Analysis, FTA)、人機系統可靠度分析(Man-Machine Reliability Analysis)、事件樹分析、人員失誤分類分析(Human Initiated Fault Analysis, HIFA)、及人員次系統測試與評估(Personnel Subsystem Test and Evaluation, PSTE)等。在安全性管理中，主要是運用資料庫工具來收集、分析數據的，它與可靠度管理、維護度管理等工程管理項目，一起作為管理工程或系統工程中的重要內容。

3.1 系統安全計畫

3.2 系統安全工作

3.3 系統安全時程與成本

3.4 產品安全需求確認

3.5 系統安全計畫監督與報告文件

4 人因工程

人因工程(Human Factor Engineering)又稱為人體工學，在歐洲國家如英國、荷蘭、法國等，使用 Ergonomics，由 ergon 及 nomos 兩個希臘字複合構成的，ergo 表示工作、nomos 代表法則或習慣(law or habit)，所以複合詞的含意是指「應使機械設備的設計符合人的工作或操作的習慣」。日本稱為人間工程或直接用 ergonomics 的譯音。美國學者認為本項學門應突出人的因素，並要把它建立在以解決實際問題為主的方法應用上，所以稱之為人員因素工程或人因工程(Human Factor Engineering)，有時亦稱為人

中国可靠性网 http://www.kekaoxing.com

員工程(Human Engineering)、工程心理學(Engineering Psychology)、系統心理學(System Psychology)。

從工業工程與工業管理的專業觀點，人因工程主要是研究探討人員的角色，為了將生產系統中的作業人員緊密地與作業所使用的工具、作業環境聯結在一起，成為一個「人-機-環境」的系統加以考慮，以人員為主導因素，使人員能舒適、健康、安全、高效率地工作，達到人機最佳配合，進而發揮提高系統效率。

人因工程的開創其實遠落後於其他工程領域，直至第二次世界大戰後才逐漸由美國軍醫方面向外擴散。由於其發展時間還不長，各學者專家對其定義與範圍仍有些許差異。但是，至少人員工程可以說是在進行工程設計時將一切有關人的因素考慮進去時，所發展出來的工程設計方法。因此，人因工程也是將人，不論與工程設計的系統有何互動，都視為工程系統中的一部分，成為必須考慮的因素。

人因工程的發展過程自有其脈絡，最主要的就在於提高生產力，大致可分為三個階段，第一階段是心理學的技術應用階段，主要是研究人如何適應機器，也包括環境、工作性質等，心理學技術廣泛地應用於工業、國防等領域，人逐漸成為人-機-環境系統中的一個重要因素，它的主要任務是挑選、培訓人員，使之適應機器的需要，算是人因工程的孕育階段。

第二階段是工程心理學的誕生階段，1940、1950 年代心理技術應用迅速發展成為一種綜合性科學，1960 年代因進步主義的抬頭，與所謂行為科學、心理學的再度結合，而獲得極大的進展與鼓舞（提高生產力上），由於 1960 年代是變化的時代，1970 年以後人員工程就有所調整了，從生產者的使用工具，轉向使用者的（消費者的）使用產品（使用產品），確定「使機器設備的設計更適合於人的使用」，不僅是要培訓人員去適應機器和讓人能夠操作的心理技術考量，同時必須轉變成「技術適應於人員」和「讓人能夠有效的操作」的角度出發，研究重點轉移到各種顯示設備，操縱機構的旋鈕、把桿、按鍵等方面，以適應人的心理生理特點。在此階段實際上開始重視人-機-環境系統的研究，所以說是人因工程的誕生階段。

第三階段是人因工程成為獨立學門的階段，重點從使「機器設備的設計更適合於人的使用」進一步發展，進入「人機系統最佳組合」的系統研究工作，考慮整個系統的效率問題，如系統的輸入輸出、回饋系統、系統功能分配、系統安全性與可靠度評價、人機系統的局部最佳配合(界面設計)、系統整體最優化選擇等課題。

1980 年代發展出所謂親人性設計或人因工程在設計上的應用等研究項目來。到了 1990 年代則更進一步發展出所謂同步工程（實作操作與模擬操作的同步），乃至所謂感性工程、省能產品與使用後評估等概念。

從字面上來說，「人因」可被理解為「人類因素」，意思是設計產品時除了要考慮產品可以提供什麼功能之外；更要考慮人類有限的能力是否足以有效地使用產品。人因工程在過去數十年中，已經幫助許許多多工程領域設計與製造出更多更的產品，小至電話鍵盤、個人電腦的軟體介面與外型，大至飛機的操作介面與機組員的互動設計(人機介面)、核電廠的操作，在許多失敗案例後借助人因工程的改良，可以使安全性與效率或附加價值大幅提高。

在國內，雖然人因工程早已廣泛應用於各工程領域，但是不論業界或學術界都偏重於安全衛生與人機系統的研究；其他方面的研究較少，如人體計測、生物力學、工

中国可靠性网 http://www.kekaoxing.com

作生理、人員績效與可靠度、人類訊息處理與決策行為、產品與環境設計、視覺與色彩等,

人因工程是研究與應用人性因素的學門，它是以人性心理學與生理學為基礎，應用於產品、系統的設計上，因此人因工程專業人員必須具備心理學，生理學，認知心理學、生物力學、工業工程、作業研究、行為科學的知識，並理解工業設計的應用方法。」

人因工程雖是一門最後可能訴諸於數字化的科學數據，但它的基本概念卻是人性因素。美國人因學會（Human Factors Society）所發表的人因工程定義：「人性因素是所有可應用於系統與產品的規範，設計，評估，操作，與維護等，以提高其安全性、效率、與滿意程度的有關人的行為與生理上特徵的科學與技術」，並且在人因學會 1992 年鑑中也清楚呈現，美國人因工程學會會員的學歷是以心理學背景佔最多 45%，其次才是工程 19.1%。那為何我們所思考的人員工程竟都是一堆人體尺寸數據，甚至僵化的相關的機具尺寸？這必須從人因工程的目的論來看，人因工程雖然以心理生理相關學門為基礎，但卻是以追求更高的工作效率為目標，在強調生產的工業化社會，這是非常重要的，所以從美國人因學會（Human Factors Society）所發表的人因工程定義中也可看出其「…安全性、效率、與滿意程度」背後的目的論。所以人因工程很難變成一種創造性的工作，因為它的目的太清楚，所以目前生理科學對人類基本能力的認識及認知，科學對感覺系統及人類資訊處理的能力，皆用來支持一種有效率的身體姿態。所以人因工程也在創造身體，創造一種有效率以生產某種意識下的工具。

4.1 人因工程在工業工程與管理領域中的地位與作用

在人因工程學門確立之前，人們已對工業管理中的人-機-環境系統進行了研究，並從中發現了一些基本原理。這些原理不僅十分有研究價值，而且可以直接應用於工業管理，提高生產系統的效率。如今，人因工程已經發展成為工業工程與管理中不可少的專門學問。造成這種發展，主要是工業生產中三方面的需要。

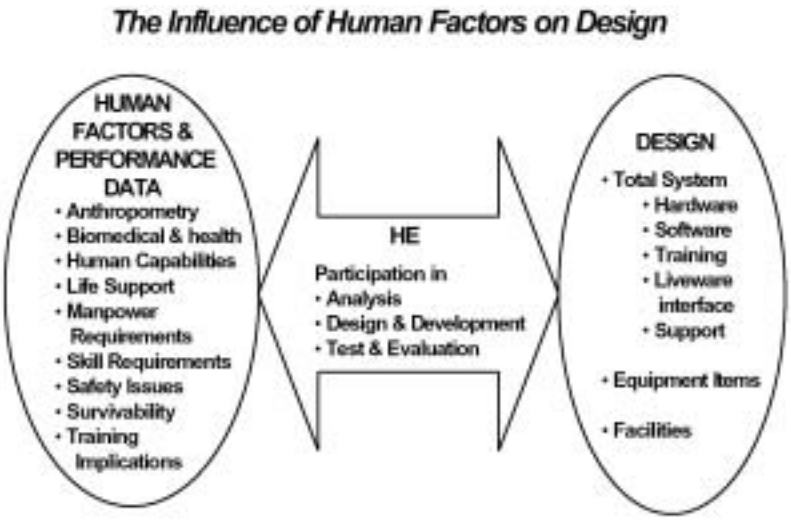
(1). 生產作業管理的需要

為了有效管理生產作業，工作場地的佈置，工作環境的照明、色彩、噪音、粉塵、溫度、濕度、通風等條件，生產線中機器與工作位置的佈置，設備、儀器、控制器的設計，工作台面工具與零組件的安放規劃，工廠人員密度、換班方式、休息時間、資訊回饋方式與管道，作業方法改善，動作時間研究等，都是與工作效率有密切的關係。工業工程管理過去雖然對這類問題有過研究，但人因工程卻提出了系統的研究方法與方析結果，並不是靠零碎的經驗與推理得到的，而是實驗或長期實踐總結而得到的完整的知識體系。因而建立了生產作業管理效率研究，用於生產作業管理的特定研究領域。

(2). 人力資源管理的需要

中国可靠性网 http://www.kekaoxing.com

(3). 標準化管理的需要



圖：人因對設計的影響

4.2 人因工程範圍

一般而言，人因工程的範圍可說相當廣，在人因工程的應用方面，通常是集合了工程、心理、與生理各方面的專家的團隊合作，至少包含有：

1. 人體工學：考量人體工作時的姿勢等，避免讓人做出有害健康的動作，或是設計使人可以在舒適的環境中工作。
2. 人體計測(Anthropometric)：對不同種族性別的人體各部位長度尺寸了解，作為設計機器位置與尺寸之用。
3. 人的決策機制：對資訊處理與判斷的機制，在危險時特別重要。所以要針對各種危險情境考量人機的互動。
4. 人機介面：包含各種控制裝置、顯示裝置與手工具的設計等。這些都必須要考量人類的生理感官與心理認知特性：
5. 人人介面：人與人的互動，在需要分工合作的系統上，也是非常重要的。例如，社會心理學在工程系統中的應用。
6. 工作環境：照明、溫度、空氣品質、噪音、震動等，都會影響人的表現與行為，因而可能誘發造成危險的因素。

中国可靠性网 http://www.kekaoxing.com

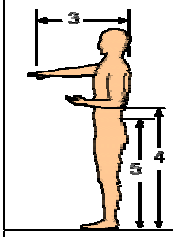
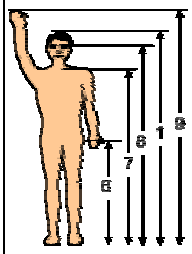
4.3 人體計測

基於人體計測資料對於日常生活與工作上的重要性，因此自第二次世界大戰以來，世界各先進國家莫不大力著手進行其國民各種特定人口，如一般人民、軍人、空服員、勞工及移民的人體計測資料庫之建立。近年來，由於歐洲聯盟（原歐洲共同體）經濟與政治上的整合與各國交流的頻繁，人體計測資料庫更廣受重視，國際標準組織（ISO）亦已將其列為標準。簡言之，人體計測資料庫之完備及其應用之普及程度，不僅可以代表一個國家的發展水準，也代表一個國家的實質生活品質。

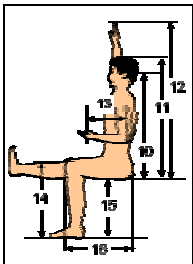
目前世界上已有九十多個大規模的人體計測資料庫，其中歐美國家佔了大部份，亞洲國家約有十個，而日本佔了一半以上，然而我國僅有中小型人體計測資料庫，不足以因應實際應用所需。近年來，我國政府單位亦陸續有系統地規劃人體計測資料庫的建立與應用，在民國 82 年與 83 年第 14 次及第 15 次行政院科技顧問會議中，均將本土化人體計測資料庫的建立與應用列為重要議題。

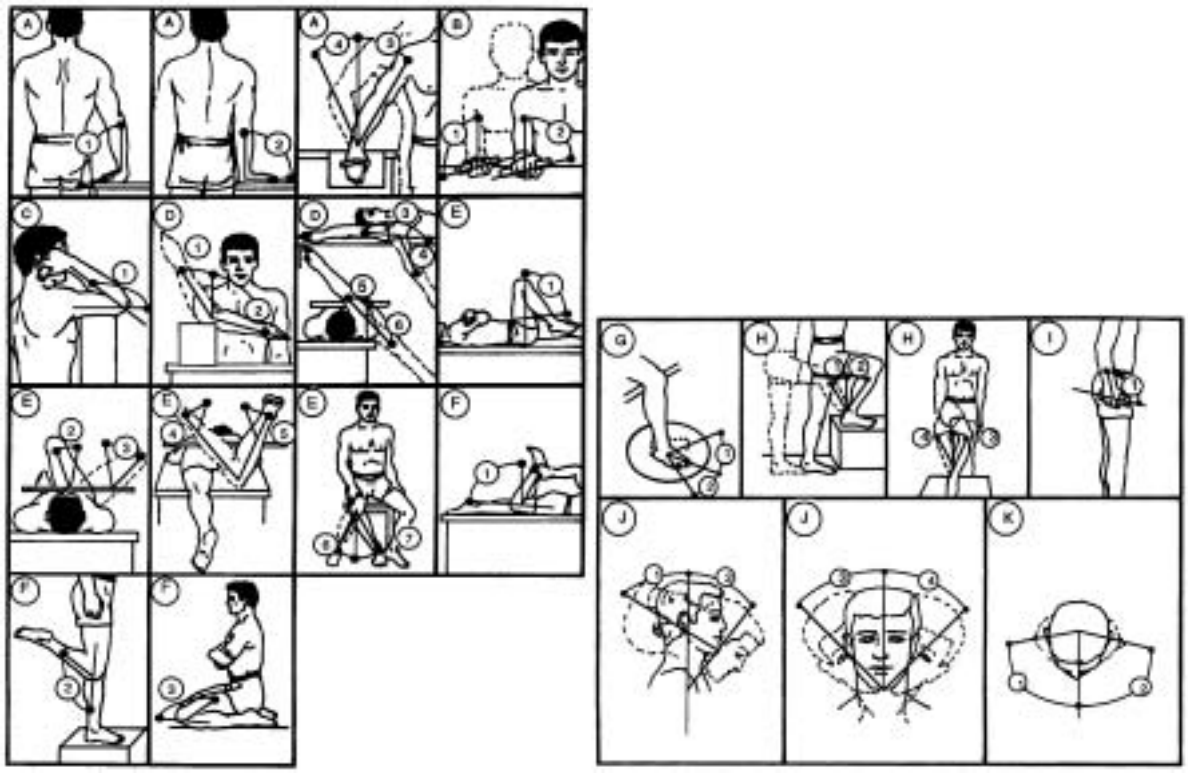
雖然在過去近二十年，國內曾陸續完成近十個人體計測資料的調查，然而由於經費限制，人力及物力不足，因此或因樣本太小、或因代表性不夠、或因量測項目太少，在設計應用時，常有不敷使用之感。基於此，行政院勞工委員會勞工安全衛生研究所於民國 82 年開始推動勞工人體計測資料調查規劃與量測，分 3 年實施，並委請國立清華大學執行，結合國內 9 個大學人因工程界研究人員共同參與。依台灣地區人口結構計取樣約 1200 位勞工，進行 266 項靜態尺寸與 42 項動態活動角度量測。表 1 是台灣常用的重要人體計測尺寸。

表 1 常用的計測尺寸（單位：mm）

量測項目			男性		女性	
			平均值	標準差	平均值	標準差
	2	體重	67.35	8.90	54.22	8.16
站姿側視圖 	3	手臂伸長距離	822.11	37.62	755.10	34.97
	4	肘高	1048.77	41.28	973.44	37.60
	5	肚臍高	990.22	44.91	910.35	43.42
站姿正視圖 	1	身高	1687.73	59.75	1563.05	53.88
	6	中指指節高	750.77	32.42	704.51	32.68
	7	肩高	1382.36	53.26	1278.86	48.35
	8	眼高	1570.01	59.26	1449.92	53.04
	9	手臂向上伸直指尖高	2103.73	84.98	1925.50	72.66
坐姿側視圖	10	眼睛至座面距離	785.34	30.89	731.79	30.81

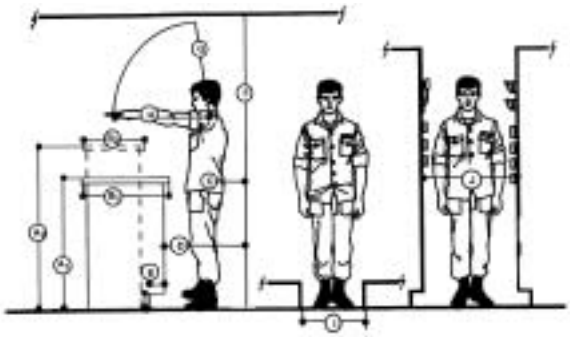
中国可靠性网 http://www.kekaoxing.com

	11	頭頂至座面距離	903.04	31.87	844.52	31.25
	12	手臂向上伸直指尖至座面距離	1322.03	54.61	1211.6	46.59
	13	手肘至握拳中心距離	306.00	27.07	271.27	23.82
	14	膝上緣高	515.66	27.69	467.06	22.19
	15	座高	404.52	19.85	376.27	15.85
	16	座深（以膝前緣至臀後緣距離估算）	551.50	32.93	526.79	26.21
頭部	17	頭長	188.71	8.18	179.06	7.72
	18	頭寬	154.17	10.26	144.60	10.46

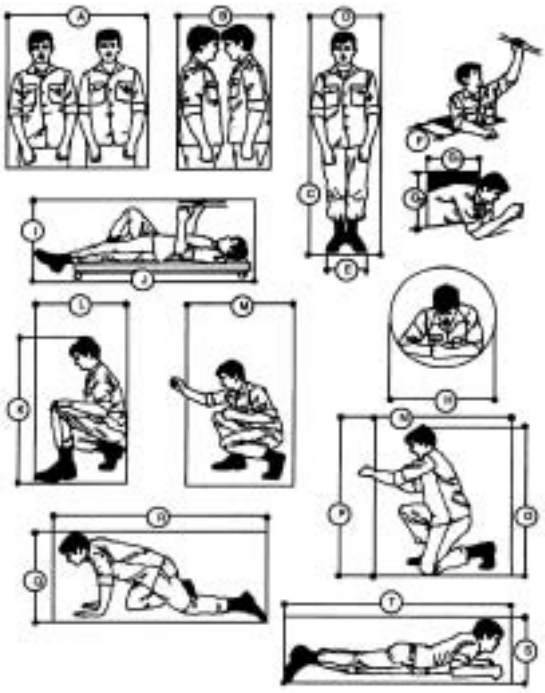


圖：人體運動範圍

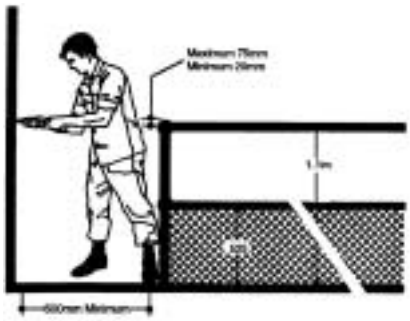
中国可靠性网 http://www.kekaoxing.com



圖：站立工作空間尺寸

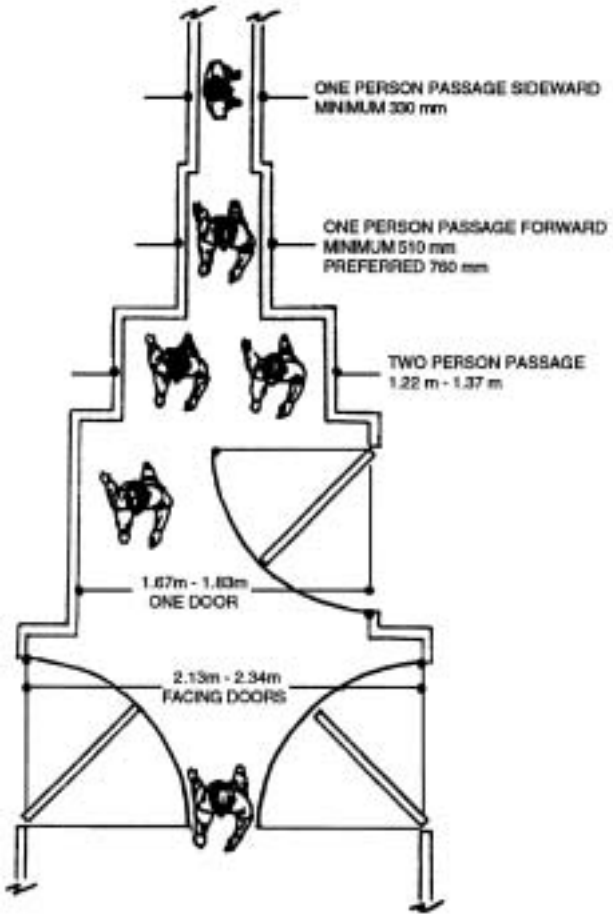


圖：運動空間尺寸

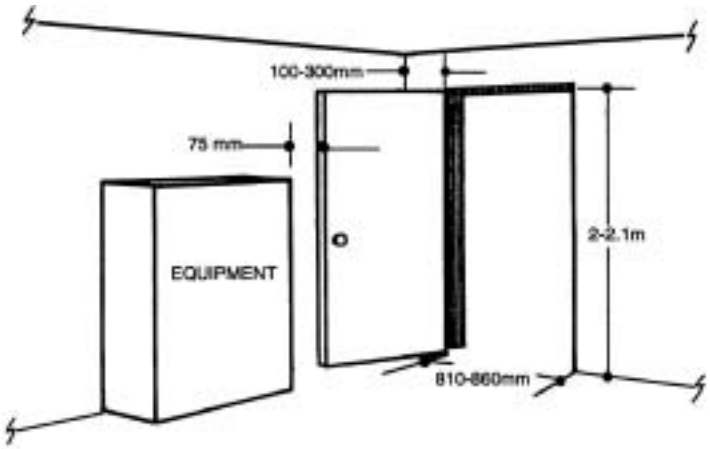


圖：扶手欄干尺寸

中国可靠性网 http://www.kekaoxing.com



圖：走道通道尺寸



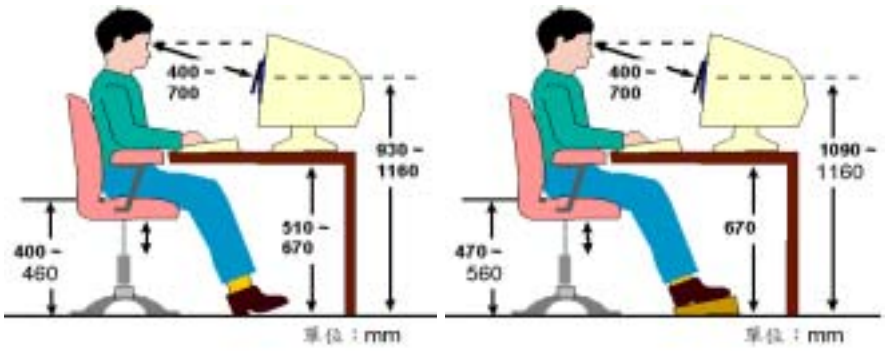
圖：門尺寸

中国可靠性网 http://www.kekaoxing.com

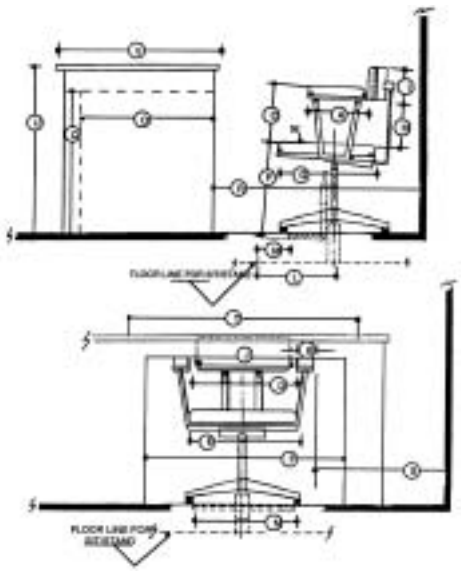
4.4 工作桌

隨著科技的進步與發展，電腦顯示終端機作業已成為許多人生活的一部分，並普遍地存在於各行業。依據本所調查研究顯示，民國 84 年底我國個人電腦的累積量已達 160 萬台。長時間電腦顯示終端機作業，容易引起眼睛乾澀(52.8%)、疼痛(33.9%)等視覺問題及上肢痠麻、僵硬等骨骼肌肉系統傷害(52.2%)。電腦顯示終端機作業引起的上肢傷害日益受到重視，美國聯邦陪審團判決，電腦製造商迪吉多公司應給予三位因操作電腦鍵盤而遭致手腕、手臂永久傷害之婦女，近六百萬美元之賠償。為預防此類傷害，勞工安全衛生研究所位針對電腦顯示終端機作業進行系列研究，以提供一適合國人體型之電腦工作桌椅尺寸設計參考值，協助電腦顯示終端機使用者調整其工作站以預防此類骨骼肌肉酸痛。

目前關於電腦工作桌椅尺寸建議值，主要是依據人體計測尺寸，考慮生物力學、工作生理學及心物法原則來訂定。早期規範著重在以"直立"的坐姿工作姿勢，亦即三個 90 度姿勢。此一姿勢下，肘、膝及臀部關節約維持在 90 度。然而關於電腦工作站的工作姿勢設定有許多不同的見解，也沒有一種完美的坐姿工作姿勢存在(例如，降低座椅高度可以使下肢得到休息，但同時也將增加上半身之負荷)，同時任何一種靜態的姿勢維持一段時間之後將會引起疲勞。因此，工作中，適時改變姿勢才是減少疲勞的好方法。就姿勢而言，一般顯示器的畫面上端應低於眼高，使臉正面朝向前方並稍稍往下，以減少因抬頭造成頸部負荷。作業時，應儘量使眼睛朝正面往下，以減少眼睛疲勞。由於人體尺寸具有很大的變異性，電腦工作站最好採取可調式的設計，而且各部份必須可以單獨調整。有時基於工作場所及經濟考量，採用固定桌面高度或坐面高度的設計，此時往往將固定高度設定在較大尺寸值，提供腳踏板以符合較小尺寸者的需求。建議的可調式及不可調式電腦工作桌椅尺寸參考值如下圖所示。



中国可靠性网 http://www.kekaoxing.com



圖：座位空間尺寸

4.5 立姿工作

目前國內家具或工作場所的設備，很多是進口的或是參考國外尺碼來設計。原因是我國尚未有一套完整的人體計測資料庫，以及設計參考值。使用不符人體計測資料的設備往往會引起疲勞。就以立姿工作桌面而言，例如廚房的流理台、浴室的洗臉盆、工廠的輸送帶等的高度都跟立姿工作桌面高度設計有關。桌面太高時，使用時必須抬舉肩膀，這樣會導致頸肩酸痛。桌面太低時，使用時必須彎腰，如此下背部會酸痛。目前一般家庭的工作桌面普遍過低，所以家庭主婦在廚房工作時，往往容易腰酸背痛。但是一般工廠的工作桌面高度往往太高，導致我國勞工反應頸肩酸痛的比例比國外高。立姿工作桌面高度設計，必須考慮立姿時手肘高度、工作種類與個人喜好。一般將工作種類分成粗重、輕度與精密作業三種。粗重作業需要較大的施力，通常工作桌面高度設定在低於手肘高度約 15-20 公分。精密作業眼睛負荷較高，工作桌面高度設定在高於手肘高度約 5-10 公分。一般輕度作業則低於手肘 10-15 公分。圖 2 是參考我國勞工人體計測資料庫所設計之三種固定式立姿工作桌面高度。由於人員高度不同，有時將工作面高度設定在較高尺寸(95 th)，提供墊子以作為較小尺寸者調整高度至工作面高度。圖 3 是以精密作業為例，將工作面高度設定在第 95 百分位男性高度，提供墊子作為較小尺寸者調整高度至工作面高度。

中国可靠性网 http://www.kekaoxing.com

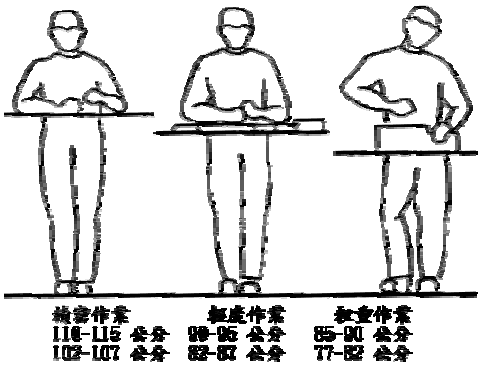


圖 2：

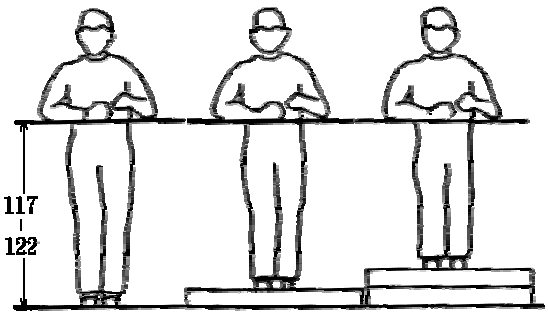


圖 3：

4.6 人因心理學

人因心理學的起源及發展

人因心理學起源於二十世紀初，於二次世界大戰期間急速發展。大戰期間，心理學家發現即使是經過嚴格訓練的軍隊人員，在操作軍器時仍難免在最基本的步驟上出錯。心理學家歸咎於機器的設計未能配合人類的認知能力，並提倡要設計機器變得更易用。自此人因心理學即被廣泛應用於軍事、國防及太空事業之上。

時至今日，人因心理學的應用範圍越來越廣泛，改善了不少家居電器與用品的設計。九十年代中期，資訊科技發展一日千里，人因心理學更被應用於改善電腦介面與網頁設計之上，為不少電子商貿網頁減少了因瀏覽者不擅操作網頁介面而錯失的商機。

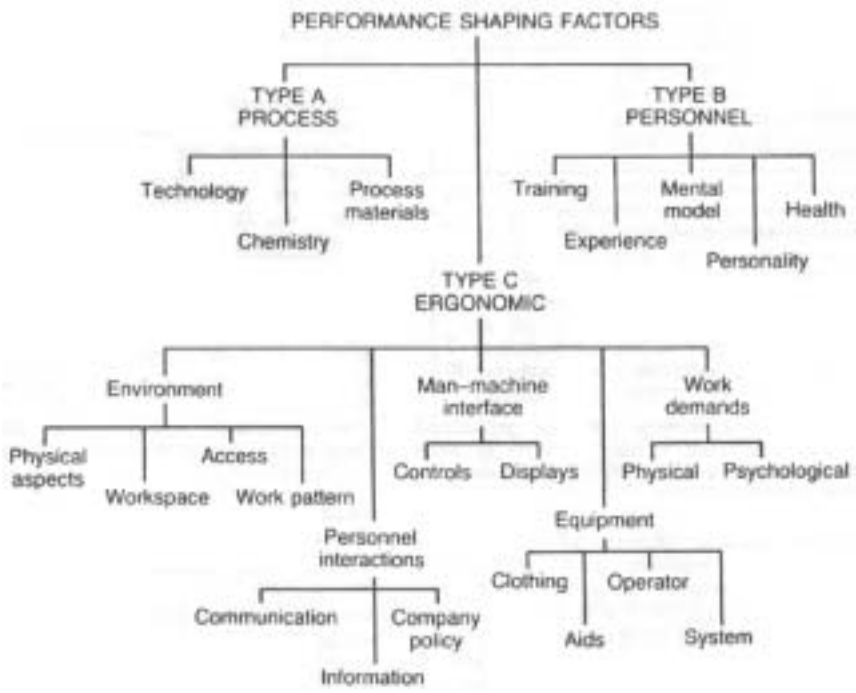
人因心理學 (Human Factors Psychology) 為心理學的一支，旨於探討人與機器的交互作用 (Man-Machine Interaction)，發展理論去預測人類使用機器時的行為模式，並從心理學的理論中研究出改善產品設計的方法，使產品的設計配合人類認知能力的限制，從而變得更易於使用。

4.6.1 人為失誤

系統發生事故的原因是安全性管理中研究歷史較長的一個主要內容，系統事故的發生是由於系統安全效能降低、亦即危害性增大所致。根據事故的直接受害對象可分為財物破壞、人員傷亡、與人機系統聯結的中斷三類。

造成事故的直接原因不外乎兩大類：人員的原因或物品的原因；而間接原因則從人與物兩方面分析，分為技術、教育、素質、管理、設計、環境等。

中国可靠性网 http://www.kekaoxing.com



4.6.2 人為失誤在事故發生過程中地位

4.6.3 人為操作失誤與系統設計不當

4.7 人員注意力問題

4.7.1 不注意

(1). 是不注意引起的事故嗎

(2). 不注意是結果不是原因

中国可靠性网 http://www.kekaoxing.com

(3). 不注意與注意

4.7.2 注意的心理構成

日本學者對注意的各種特性進行評價測驗後曾指出，注意只是構成各種心理活動的過程，而作為一種具有組織化機能表現出來的特性，是基於媒介物和間接性的一種狀態。

一般認為，人的大腦皮層在普遍具有一定興奮水平時，即覺醒狀態的基礎上，由於某些特定刺激的影響，可以在相應的區域內形成一個優勢興奮中心。此時，

4.7.3 注意的生理基礎

5 作業環境

5.1 氣候環境

中国可靠性网 http://www.kekaoxing.com

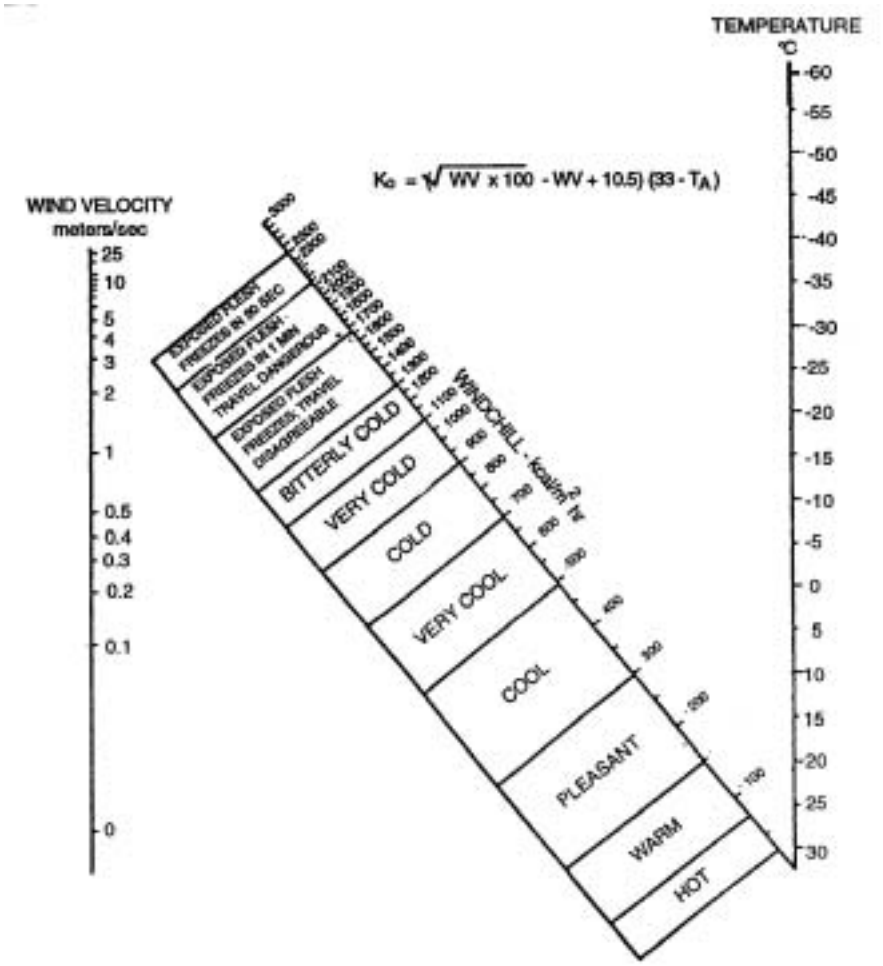
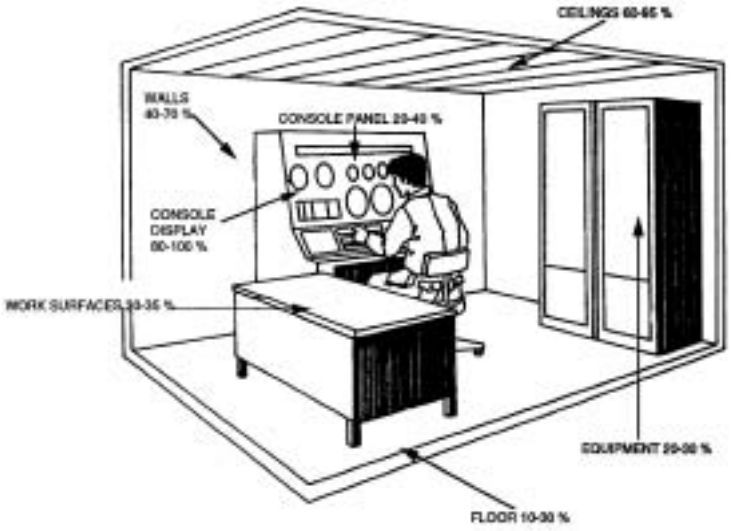


圖 10：風激冷圖表

5.2 照明環境



中国可靠性网 http://www.kekaoxing.com

圖：工作空間表面反射數值

5.3 振動環境

5.4 噪音環境

6 危害分析技術

系統工程中針對系統危害的分析方法，一般而言有下面幾種：

1. 邏輯分析
2. 機率可靠度
3. 失誤樹分析(Fault-Tree Analysis)：或譯為故障樹分析
4. 統計分析
5. 系統可靠度分析

其中的機率可靠度、系統可靠度分析、統計分析等方法多用於可以量化的問題中，特別常見於生產線上的研究課題中，失誤樹分析基本上可以視為邏輯分析的一種，特別用於多層次的問題分析中。

6.1 初步危害分析

6.2 失效危害分析

中国可靠性网 http://www.kekaoxing.com

7 危害分析與安全驗證

7.1 危害種類

7.2 安全驗證

7.3 消費性產品不合理危害試驗

8 軟體系統安全

8.1 軟體系統安全手冊

系統安全協會（SSS）近期公佈了有關系統安全的幾個標準和檔案，包括 DOD 系統安全性標準實踐 MIL-STD-882D（2000 年版，替代 1993 年版 MIL-STD-882C）、軟體系統安全手冊和 DOD 設計規範標準人力工程 MIL-STD-1472F。

軟體系統安全手冊是由聯合服務電腦資源管理工作組和美國海軍、陸軍、空軍在電子工業協會（EIA）G-48 委員會和聯合服務系統安全小組所屬的聯合服務軟體安全委員會的指導下投資和開發完成的。介紹現在，數位電腦系統在幾乎所有商業和政府的主要技術中都充當起關鍵性安全功能自動控制的角色，這一革命的主要原因就是軟體能夠以人力無法達到的速度可靠地完成關鍵控制任務。因此，在安全關鍵性系統中進行系統安全工程工作以降低系統風險就顯得尤為重要。軟體系統安全性（SSS）活動作為系統安全工程任務的一部分，主要包括設計、編碼、測試、獨立確認與驗證（IV&V）、操作與維護和軟體工程開發程序控制功能改變等。

由聯合服務電腦資源管理工作組和美國海軍、陸軍、空軍開發完成的這一軟體系統安全手冊（以下簡稱手冊）的主要目的是：提供管理和工程導則，實現合理的保證等級，保證軟體以可接受的安全風險等級在系統環境中運行。該手冊（SSSH）是聯合

中国可靠性网 http://www.kekaoxing.com

工作的成果，美國陸軍、海軍、空軍和海岸防衛安全中心與聯邦飛行管理部門（FAA）、NASA、國防工業承包商以及學術界都作了很多工作。

8.1.1 範圍

該手冊是為幫助政府或行業組織的各個層次的管理人士和工程人員提供參考文檔和管理工具。它論證的是開發和實現有效 SSS 過程的“如何”問題。該手冊所提出的 SSS 任務、技術和過程對在關鍵領域使用軟體的任何系統都是一個足夠的基礎。該手冊給出了為保證由軟體控制的硬體系統的安全性而需要理解和應用定性和定量分析技術所用到的學科。

該手冊起到的是一個指導作用，而不是要替代適用於系統安全性或軟體工程與開發的任何機構的政策、標準或導則，如 MIL-STD-882D（C）、MIL-STD-498。編寫該手冊的目的是為了闡明政府和商業標準及導則檔中的 SSS 需求和任務。雖然該手冊不是關於軟體工程的指南，但它確實也給出了一些軟體功能和設計方面的技術問題來幫助理解軟體安全性。

該手冊的目標之一是向每一個 SSS 工作組的成員提供一個對可靠系統和軟體安全性實踐的基礎理解。而另外一個目標則是證明在定義安全關鍵性軟體部件的系統軟體安全需求中，每一項技術和管理科目對聯合工作的重要性。最終的目標是給出可以在哪里將安全特性設計到軟體中去，以消除或控制識別到的風險。

8.1.2 組織結構

該手冊共有五大部分的內容，包括：

1. 執行概要

第一部分給出了手冊執行概要，向執行管理人員提供了關於軟體安全性的簡要目標概述，同時傳達了 SSS 專案的需求和典據；需求的動機和典據；以及對用戶、專案、設計和開發工程準則的作用和責任。這一部分可能是執行官、專案經理或 PM 唯一所需的部分，以確定他們的專案中是否需要軟體安全性專案。

2. 介紹

第 2 部分給出了手冊的深入描述和手冊的目的與範圍，以及手冊編排描述和它在系統開發的採辦壽命週期中的應用。

3. 風險管理與系統安全介紹

第 3 部分針對那些對 **MIL-STD-882** 方法和建立、實施 SSP 並不十分熟悉的讀者給出了系統安全性工程和管理的介紹。這一部分還提供了風險管理介紹和為什麼安全性風險是風險管理功能中所必需的部分。另外，第 3 部分還介紹並概述了系統採辦、系統工程和軟體發展過程，給出了在複雜的系統安全過程中將這些工作進行有效集成的指導。

4. 軟體安全性工程

第 4 部分解答了基礎軟體安全性專案的“如何”問題。作者認識到並不是所有的採辦和採購都是相同的，他們處理的以技術、資源、開發壽命週期和個性等方式出現的問題、假設和限制也不盡相同。這一部分就提供了從業者建立、製作、實施 SwSSP

中国可靠性网 http://www.kekaoxing.com

導則進行仔細計畫考慮的基礎。這一部分的組織邏輯是為了給讀者提供計畫、任務實施和風險評價所需的步驟，以及一個 SSS 專案的通過接受。在附錄 C.9—11 中給出了關於配置變更的管理和屬於軟體再利用和 COTS 套裝軟體的問題。

5. 附錄

附錄 A：辭彙定義

附錄 B：參考資料

附錄 C：手冊補充資料

附錄 D：COTS 與 NDI 軟體

附錄 E：通用需求與導則

附錄 F：經驗（lessons learned）

附錄 G：合約文檔範例

中国可靠性网 http://www.kekaoxing.com

參考資料

1. MIL-HDBK-759, Department of Defense Handbook for Human Engineering Design Guidelines
2. MIL-HDBK-761, Department of Defense Handbook Human Engineering Guidelines for Management Information Systems
3. MIL-HDBK-46855, Department of Defense Handbook Human Engineering Program Process and Procedures
4. MIL-STD-882, Department of Defense Standard Practice for System Safety
5. MIL-STD-1574, Military Standard System Safety Program for Space and Missile Systems
6. MIL-H-46855, Military Specification Human Engineering Requirements for Military Systems, Equipment, and Facilities.
7. 勞工安全衛生研究所資料庫
8.

中国可靠性网 http://www.kekaoxing.com