與品質管理有關的工具、方法、技術及其應用

ISO 31010

CNS 31010

Risk management – Risk assessment techniques

風險管理－風險評鑑技術

目　錄

5. 風險評鑑過程

5.1 一般

5.2 風險鑑別

5.3 風險分析

5.4 風險評估

5.5 文件化

5.6 監測與審查風險評鑑

5.7 生命週期階段中風險評鑑之應用

6. 風險評鑑技術之選擇

6.1 一般

6.2 技術之選擇

6.3 資源之可取得性

6.4 不確定性之本質與程度

6.5 複雜性

6.6 生命週期階段中風險評鑑之應用

6.7 風險評鑑技術之類型

附錄A(參考)風險評鑑技術之比較

附錄B(參考)風險評鑑技術

參考資料

前言

本標準係依據2009年發行之第一版IEC/ISO 31010，不變更技術內容，制定成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

前言

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

所有類型與規模的組織面臨許多可能影響其目標達成的部分程度風險。

此等目標可能與組織的活動範圍有關，由策略性創議至其營運、過程及專案，且反映在社會、環境、技術、安全與保全的成果，商業、財務及經濟的策略，以及社會、文化、政治及聲譽影響之形式上。

組織所有活動涉及風險，須予以管理。風險管理過程有助於透過考量不確定性與未來事件或狀況(預期的或未預期的)之可能性，及其對既定目標之影響，以制定決

簡介

風險管理包括運用邏輯化與系統化的方法，用以：

- 在整個過程期間進行溝通與諮商。
- 為鑑別、分析、評估、處理與任何活動、過程、部門或產品有關的風險建立前後環節。
- 監測與審查風險。
- 適當地報告並記錄後果。

風險評鑑為風險管理之一部分，此一部分提供結構化的過程，用以鑑別目標可能如何地受到影響，並在決定是否需進一步

簡介

處理前，先以後果(亦稱結果，以下統稱為後果)與其機率(亦稱或然率，以下統稱為機率)之形式分析此風險。

風險評鑑試圖回答下列基本問題。

- 可能發生何種情況及其理由(藉由風險鑑別)？
- 後果為何？
- 其將來發生的機率為何？
- 是否有減輕風險後果或降低風險機率的任何因素？

風險之等級可否容忍或接受，以及其是否

簡介

需進一步處理？本標準試圖反映風險評鑑技術之選擇，與利用目前的良好實務，並不討論尚未達成專業共識滿意度的新或進展中的概念。

本標準本質上為一通用性標準，可提供跨型式產業與系統類型之指導。在這些產業中可能已有更特定的標準，為特殊應用而制定合宜的方法與評鑑之水準。若此等標準與本標準調和，則該等特定標準一般而言已足敷應用。

1. 適用範圍

本標準係CNS 31000之支援標準，並對風險評鑑系統化技術的選擇與應用提供指導。

依據本標準進行風險評鑑有助於其他風險管理活動。

介紹系列技術之應用時，已明確參照其他國家(國際)標準，其中對技術之概念與應用有更詳細的描述。

本標準無意作為驗證、法規或合約目的使用。

本標準不提供鑑別風險分析需求之明確準

方法之型式。

本標準並未提及所有技術，本標準所遺漏之技術，並不意味該方法無效。將此方法應用於某一特殊狀況，實際上並不意味必須應用此方法。

備考：本標準未特別論及安全。本標準為一般的風險管理標準且任何安全之參考資料純粹為參考性質。有關安全考量面已納入ISO/IEC Guide 51。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括

補充增修)。

CNS 14889　風險管理－詞彙

CNS 31000　風險管理－原則與指導綱要

3. 用語及定義

CNS 14889所規定之用語及定義適用於本標準。

4. 風險評鑑概念

4.1　目的與效益

風險評鑑之目的為提供經求證的資訊和分析，以便在如何處理特定風險，以及如何就選項進行選擇方面，做出具充分資訊的

決策。實施風險評鑑的一些基本效益包括：

- 瞭解此風險及其對目標之潛在影響。
- 提供決策者資訊。
- 有助於瞭解風險，以協助對處理選項之選擇。
- 鑑別系統與組織中風險與脆弱環節之重要貢獻。
- 比較替代系統、技術或方法中的風險。
- 溝通風險與不確定性。
- 協助建立優先順序。
- 以事故事後調查後果，協助事故之預

- 選擇不同的風險處理方式。
- 符合法令規章要求。
- 與預先界定的準則相比較，提供協助評估此風險是否須予以接受之資訊。
- 評鑑最終處置之風險。

4.2 風險評鑑與風險管理架構

本標準假設風險評鑑係在CNS 31000描述的風險管理架構與過程範圍內實施。

風險管理架構提供可將風險管理深植於全組織所有階層的政策、程序及組織的規劃。

作為此架構之一部分，組織須具有政策或

特別的是，執行風險評鑑者須清楚有關下列事項。

- 組織的前後環節與目標。
- 可忍受的風險之程度與類型，並對無法接受的風險如何予以處理。
- 如何將風險評鑑整合於組織的過程中。
- 風險評鑑所使用的方法與技術，以及對風險管理過程之貢獻。
- 執行風險評鑑的當責、職責及職權。
- 實施風險評鑑所可利用的資源。
- 風險評鑑如何予以報告與審查。

4.3 風險評鑑與風險管理過程

4.3.1 一般

風險評鑑由界定於CNS 31000標準的風險管理過程之核心要項所組成，並包括下列要項。

- 溝通與諮商。
- 建立前後環節。
- 風險評鑑(由風險鑑別、風險分析及風險評估組成)。
- 風險處理。
- 監測與審查。

風險評鑑並非一獨立活動，須完全整合於風險管理過程其他組成要項之中。

4.3.2 溝通與諮商

成功的風險管理依賴與利害相關者有效的溝通與諮商。

邀約利害相關者參與風險管理過程將可協助：

- 擬定溝通計畫。
- 適當地界定前後環節。
- 確保利害相關者之利益已予以瞭解並考量。
- 聚集不同領域的專家以鑑別與分析

風險。

- 確保於評估風險時已適當地考量不同的意見。
- 確保風險已充分地鑑別。
- 確保處理計畫的獲得認同與支持。

利害相關者須有助於風險評鑑過程與其他管理職能，包括變動管理、專案與方案管理，以及財務管理等之介面。

4.3.3 建立前後環節

建立前後環節可界定管理風險的基本參數，並設定整個過程的範圍與準則。建立前後環節包含考量與全組織相關的內部與

外部參數，以及擬予以評鑑的特定風險之背景。

在建立前後環節時，將決定並同意風險評鑑目標、風險準則及風險評鑑方案。

對一特定的風險評鑑，建立前後環節須包括界定外部、內部及風險管理情況，以及風險準則分類。

(a) 建立外部前後環節涉及熟悉組織與系統所處的營運環境，包括：

- 無論是國際、國家、區域或地方的文化、社會、政治、法令、規章、財務、

- 對組織目標具有衝擊影響之主要推動者與趨勢；及
- 與外部利害相關者的關係，以及外部利害相關者之感知與價值。

(b) 建立內部前後環節包括瞭解。

- 組織在資源與知識方面之能力。
- 資訊流與決策訂定過程。
- 內部利害相關者。
- 目標及用以達成目標的策略。
- 感知、價值及文化。
- 政策與過程。
- 組織所採用的標準與參考模式；及

- 結構(如治理、角色及當責)。

(c) 建立風險管理過程之前後環節包括：

- 界定適用範圍，以及風險管理活動進行的深度與幅度，包含特定涵括事項與排除事項。
- 界定以時間與地點為觀點之活動、過程、功能、專案計畫、產品、服務或資產。
- 界定特定專案、過程或活動與組織其他專案、過程或活動間之關係。
- 界定風險評鑑方法論。
- 界定風險準則。

- 界定風險管理的績效與有效性評估之方式。
- 鑑別與詳述經作成的決策；及
- 鑑別、限定或設計所需之研究、其範圍與目標，及此類研究案所需的資源。

(d) 界定風險準則包括決定：

- 欲涵括的結果之本質與型式，及其將如何量測。
- 機率表示之方式。
- 風險等級如何予以決定。
- 決定風險何時需予以處理之準則。

準則。

- 是否與如何考慮風險的組合。

準則可依如下列緣由為基礎。

- 協議的過程目標。
- 規範中所鑑別出的準則。
- 一般資料緣由。
- 一般已接受的產業準則，諸如安全完整性等級等。
- 組織的風險度量。
- 特定設備或應用之法令與其他要求。

4.3.4 風險評鑑

風險評鑑係風險鑑別、風險分析及風險

評估之整體過程。特定個別活動或特定風險予以評鑑。不同前後環節可能適合運用不同的工具與技術。

風險評鑑提供風險、其原因、後果及機率的瞭解。風險評鑑提供有關下列決策之輸入。

- 活動是否須進行。
- 機會如何最大化。
- 風險是否需予以處理。
- 不同風險的選項間之選擇。
- 風險處理選項之優先順序。
- 可將負面風險引導至可忍受等級之風

險處理策略的最適當選擇。

4.3.5 風險處理

風險處理係指完成風險評鑑後，選擇與同意一或多個相關選項改變風險發生的機率、風險的效應，或兼具兩者，並實施此等選項。

其後再進行新風險等級的週期性重新評鑑，並依據先前設定的準則予以決定其可忍受程度，以決定是否需進一步處理。

4.3.6 監測與審查

作為風險管理過程之一部分，風險與控管

須定期予以監測與審查，以查證：

- 有關風險之假設仍維持有效。
- 有關風險評鑑所依據之假設，包括外部與內部情況，仍維持有效。
- 達成預期的後果。
- 風險評鑑後果與實際經驗一致。
- 風險評鑑技術經適當地應用。
- 風險處理展現效果。

監測與實施審查之當責須予以建立。

5. 風險評鑑過程

5.1 一般

風險評鑑協助決策者與應負責團體更進一步瞭解有可能影響目標達成的風險，及現有控管之適切性與有效性。此一功能提供有關選擇處理風險最適宜方式之決策基礎。風險評鑑的輸出為組織決策制定過程之輸入。

風險評鑑係風險鑑別、風險分析及風險評估之整體過程(參照圖1)。此過程實施之方式不僅有賴於風險管理過程之前後環節，亦與執行風險評鑑所用的方法與技術有關。

由於風險可能涵蓋範圍廣泛的原因與後

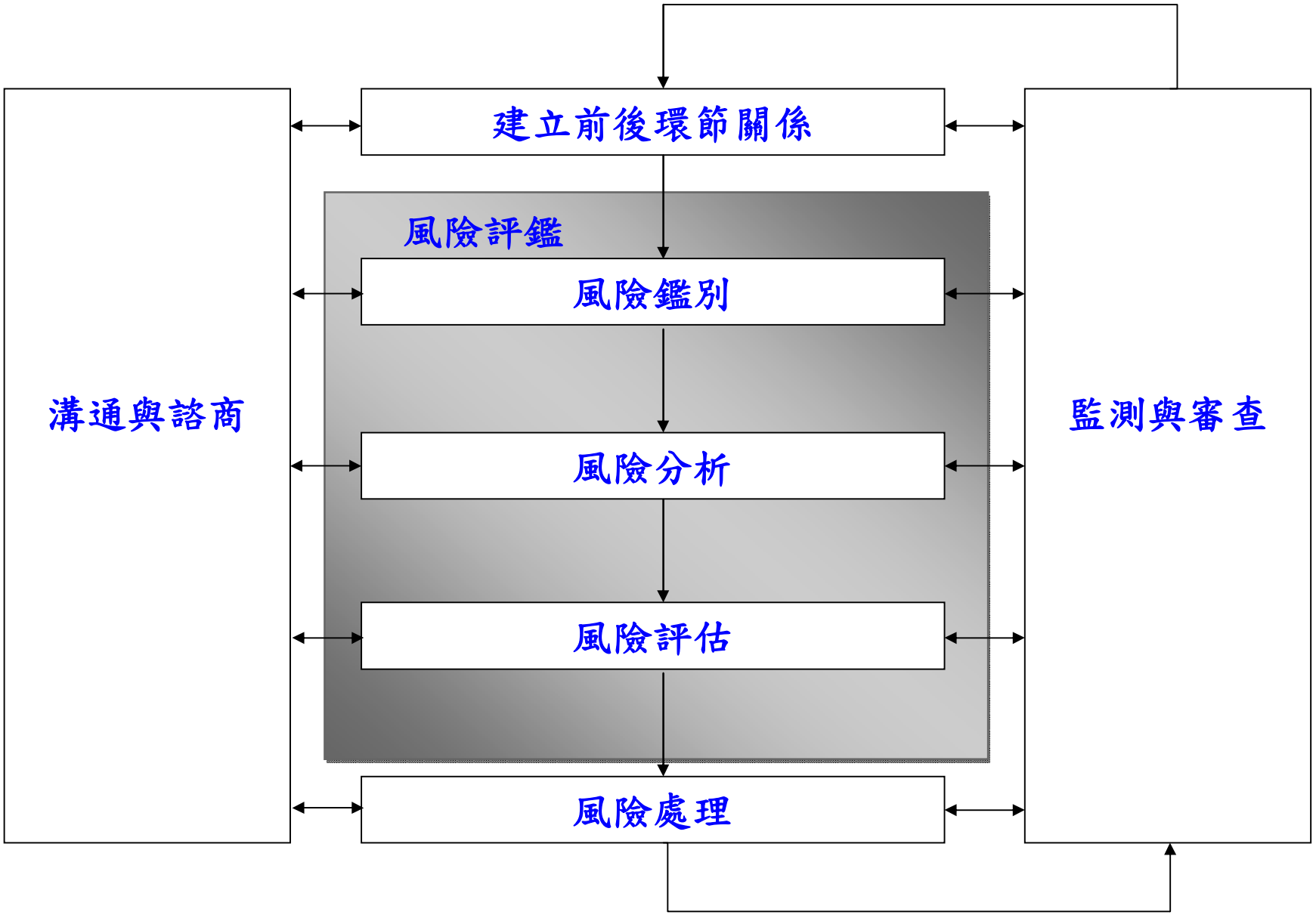


圖1　風險評鑑對風險管理過程之貢獻

5.2 風險鑑別

風險鑑別係發現、認知及記錄風險之過程。

風險鑑別之目的係鑑別可能發生或可能存在，且可能影響系統或組織目標達成之狀況。風險經鑑別出之後，組織須鑑別現有的任何控管，諸如特殊設計、人員、過程及系統等。

風險鑑別過程包括鑑別可能對目標具有實質影響的風險(人體傷害性前後環節之危害)、事件、情境或狀況的原因與緣由，以及此衝擊影響之本質。

風險鑑別方法可包括：

- 以證據為基礎之方法，範例有查檢表與歷史資料之審查。
- 系統化的小組方式，一組專家透過結構化的提示或問題組之方式，依照系統化的過程鑑別風險。
- 歸納推理技術諸如HAZOP。

可使用各種支援技術以改進風險鑑別的準確性與完整性，包括腦力激盪與德爾菲(Delphi)方法論。

不論實際所使用的技術為何，重要的是當鑑別風險時，充分地認知人因與組織因

因此，人為因素與組織因素與預期之偏差，與〝硬體〞或〝軟體〞事件一樣，都須納入風險鑑別過程。

5.3 風險分析

5.3.1 一般

風險分析係有關發展對風險之瞭解。此瞭解提供風險評鑑之輸入，並提供決定有關風險是否需予以處理，以及有關最適宜的風險處理策略與方法之輸入。

風險分析包含決定所鑑別的風險事件之後果與其機率，考量任何已有或欠缺的控管，

及既有控管的有效性，然後合併此後果與其機率以決定風險等級。

風險分析涉及考量風險之原因與緣由、其後果，及此等後果可能發生的機率。影響後果與機率的因素須予以鑑別。一事件可具有多重後果且可影響多個目標。既有的風險控管與其有效性須予以考量。此等分析之各種方法描述於附錄B。對於複雜之應用，可能須一種以上的技術。

風險分析通常包括估計可能由一事件、情況或狀況產生的潛在後果之範圍，及其伴隨的機率，以量測風險等級。然而在某些

案例中，諸如當後果可能微不足道或機率預期極低時，單一參數之估計可能足已形成決定。

在某些狀況中，所產生的後果可能係多種不同事件或情況範圍的後果，或係源自未能鑑別出之特定事件。在此情況，風險評鑑的重點置於界定有關保護或恢復策略層面之處理措施之觀點，分析此系統構成要項的重要性與弱點。

使用於分析風險的方法可為定性、半定量或定量。所要求的詳細程度依據特殊之應用、可靠的資料之可取得性及組織決策

過程之需求而定。某些分析方法與詳細程度，法令可能有所規定。

定性評鑑以顯著程度諸如〝高〞、〝中〞及〝低〞三級來界定後果、機率及風險之等級，可將後果與機率合併，並依據定性之準則評估所合成的風險之等級。

半定量方法使用數值量尺評定後果與機率等級，再以公式結合兩者產生出風險等級。量尺可以是線性或對數型，或其他型式。使用的公式亦有不同類型。

定量分析估計後果與其機率實際的數值，並產生發展前後環節時界定的特定單

風險等級數值。全定量分析可能並非經常可行或合意的，因有關所分析的系統或活動缺乏資料、人為因素的影響等，或由於定量分析的努力後果無法予以保證或要求。在此狀況下，由各別領域中博學多識的專家之比較性的半定量或定性的風險排序，可能仍為有效的。

若此分析為定性之情況，使用的所有用語須有明確的解釋，且所有準則的基準須予以記錄。

縱使已進行全定量，需認知到所計算出的風險等級為估計值。須小心確使其不致被

歸因於風險等級值之準確度與精密度與使用資料及方法之準確度不一致。

風險等級須以最適合於此風險類型之措辭，及有助於風險評估之格式表示。在某些例子中，風險大小可以機率分配於某一段後果範圍之方式表示之。

5.3.2 控管評鑑

風險等級崙視既有控管之適切性與有效性而定。須強調的問題包括：

- 對各特定風險之既有控管為何？
- 此等控管是否足以適切地處理風險，使其控制至可忍受的等級？

- 實務上，此等控管是否依預期的方式運作，且於要求時，是否可展現為有效的？

此等問題僅當具備適當的文件化與保證過程時，可以有信心地予以答覆。

對某特定控管或有關的控管配套之有效性程度，可以定性、半定量或定量之方式表示。在大多數情況中，高程度之準確性通常難以保證。然而，表達並記錄風險控管有效性之措施仍可能有其價值，得使對努力成果是否已最佳地擴展於改進其控管，或提供他種風險處理方式予以判斷。

5.3.3 後果分析

後果分析係假設已發生特定事件、情況或狀況下，決定可能產生的衝擊之本質與類型。一事件可能具有不同幅度的衝擊範圍，且影響不同範圍的目標與利害相關者。當前後環節建立後，欲分析的後果與受影響的利害相關者應業已決定。

後果分析可由簡單的後果敘述至詳細的定量模式或弱點分析予以變動。

衝擊可能會係低後果但高機率，或高後果與低機率，或某些介於中間之後果。在某些情況中，著重於可能具有極大後果的

風險較適宜，由於此通常為管理者最強烈關切者。在某些情況中，同時個別分析高與低後後果之風險可能是重要的。例如，一項經常性但低衝擊(或慢性)的問題，可能具有大的長期或累積之影響。此外，涉及此兩種明顯不同類型的風險之處理措施通常極不相同，因此對之個別分析係有用的。

後果分析可包括：

- 考量既有對處理後果之控管，連同所有對此後果具有影響的相關貢獻之因素。

- 將風險的後果關連到原始目標。
- 若與評鑑的範圍連貫時，同時考量其立即的後果與歷經一段時間後可能產生的後果。
- 考量二次後果，諸如對相關的系統、活動、設備或組織之衝擊。

5.3.4 可能性分析與機率估算

通常使用三種通用方式以估算機率，可單獨或合併使用。

(a)使用相關的歷史資料以鑑別過去曾發生的事件或情況，藉此得以外插法求得其未來發生的機率。使用的資料須

與考量中的系統、設施、組織或活動之類型相關，亦須與涉及組織之作業標準相關。若歷史資料具有極低的發生頻率，則機率估算值將極為不確定。此尤其適用於未能假設事件、情況或狀況在未來不會發生之零發生率。

(b) 使用如失效(故障)樹分析與事件樹分析(參照附錄B)等預測技術之機率預測。當歷史資料無法取得或不足時，必須透過系統、活動、設備、組織及其相關的失效或成功狀態的分析導出

經驗的數值資料，或經發布的資料緣由，合併產生頂端事件的機率估算值。當使用預測技術時，重要的是確保訂定共同失效模式的可能性分析中應有之裕度，涉及由相同原因導致的系統內一些不同組件或元件同時發生之失效。可能需以模擬實驗技術，藉由計算不確定性效應來產生因老化與其他劣化過程所致設備與結構性失效的機率之影響。

(c) 專家意見可用於系統化與結構性過程中來估算機率。專家的判斷須提出

所有相關備妥之資訊，包括歷史性、特定系統、特定組織、實驗、設計等資料。有一些引出專家判斷的正式方法，可協助提供對適宜的問題之系統化陳述。可利用的方法包括德爾菲(Delphi)法、成對比較、類別分等及絕對機率判斷。

5.3.5 初步分析

風險可予以篩選以鑑別出最顯著的風險，或將較不顯著風險或次要風險排除於進一步分析之外。目的為確使將資源著重於最重要的風險。須小心不

不致篩除經常發生且具有顯著累積影響之低風險。

篩選須依據前後環節中所界定之準則，初步分析決定下列一或多項措施途徑。

- 決定不再進一步評鑑的處理風險。
- 擱置未具處理的合理理由之不顯著風險。
- 進行更詳盡的風險評鑑。

最初的假設與後果須予以文件化。

5.3.6 不確定性與敏感度

通常有值得注意的不確定性伴隨著風險分

後果瞭解不確定性係必要的。不確定性分析結合資料、方法及模式，用以鑑別與分析風險，在其應用中扮演一重要的部分。不確定性分析包含後果中的變異或不精密度之測定，產生自用以界定後果的參數與假設之集合變異。與不確定性分析密切相關的領域係敏感度分析。

敏感度分析涉及決定個別輸入參數所改變的風險量之大小與顯著性。係用以鑑別那些需準確的資料，而那些是較低敏感者對整體準確度具有較低

影響者。

風險分析的完整性與準確度須儘可能完全陳述。不確定性之緣由可能時須予以鑑別，並須著重在資料與模式/方法兩者之不確定性。若分析為敏感者，其參數與敏感程度須予以說明。

5.4 風險評估

風險評估涉及比較估計的風險等級與於前後環節建立時所界定的風險準則，以判定風險的等級與類型之顯著性。

風險評估使用風險分析當中所獲得對風險之瞭解，作成有關未來行動之決策。

道德、法律、財務及其他包括風險感知等考量事項，亦為決策之輸入。

決策可包括：

- 某一風險是否需處理。
- 處理之優先性。
- 活動是否須進行。
- 須遵循若干途徑中之何者。

所需作成的決策之本質以及作成此等決策使用的準則，在建立前後環節時已決定，但其在此階段需更詳細視察，使更瞭解有關所鑑別出的特定風險。

界定風險準則最簡單的架構為單一

層面區分需處理與不需處理之風險。此得到受歡迎的簡單後果，但在估計風險與界定處理或不需處理之間的界限時，兩者皆無法反映所涉及的不確定性。關於是否與如何處理風險之決策，可依據接受此風險的成本與利益，以及實施改的控管之成本與利益而定。

一般方式為將風險區分為三區帶。

(a)上層區帶：無論活動可能帶來的利益為何，風險等級被視為無法忍受，且不論其成本為何，風險處理係必要的。

(b) 中間區帶(或灰色區域)：成本與利益皆予以考量且機會與可能的後果均衡。

(c) 下層區帶：風險等級被視為可忽略，或小至不需風險處理措施。

安全應用所使用的〝ALARP(最低合理可行原則)〞準則系統遵循此方式，在中間區帶，對於成本與利益可直接比較的低風險具有滑動的量尺，至於高風險，發生危害的可能性必須降低，直至進一步降低之成本與所獲得之利益完全不成比例。

5.5 文件化

風險評鑑過程須連同評鑑後果予以文件化。

風險須以可瞭解的用語表示，且表示風險等級的單位須清楚。

報告之範圍視評鑑之目標與範圍而定。除極簡單的評鑑外，文件可包括：

- 目標與範圍。
- 系統與其功能的相關部分之描述。
- 組織的外部與內部前後環節一般，及其如何關聯至接受評鑑的情況、系統或狀況。
- 適用的風險準則及其正當性。

- 評鑑方法論。
- 風險鑑別後果。
- 資料、假設及其緣由與確證。
- 風險分析後果與其評估。
- 敏感度與不確定性分析。
- 需予以監測的關鍵性假設與其他因素。
- 後果之討論。
- 結論與建議事項。
- 參考資料。

若風險評鑑支援持續的風險管理過程，執行與文件化之方式須使其可在系統、組

當顯著的新資訊成為可利用且前後環節變化時，評鑑須依據管理過程的需求予以更新。

5.6 監測與審查風險評鑑

風險管理過程將強調歷經時間預期可能變化，以及可使風險評鑑產生變化或失效的前後環節與其他因素。此等因素為進行中的監測與審查，須予以特別鑑別，以使必要時風險評鑑可予以更新。

為修改風險評鑑所監測的資料亦須予以鑑別與蒐集。

控管之有效性亦須予以監測與文件化，以提供風險分析使用之資料。建立與審查此證據與文件化之當責須予以界定。

5.7 生命週期階段中風險評鑑之應用

許多活動、專案及產品可被考量具有生命週期，由起始的概念與定義開始經由實現至最終完結，此可能包括硬體的汰除與最終處理。

風險評鑑可應用於生命週期之所有階段，且通常實施多次，各具不同的詳細程度，

以協助在每一階段所需形成的決策。

生命週期階段具有不同的要求且需要不同的技術。例如，在概念與定義階段中，當一機會已予鑑別，可使用風險評鑑以決定是否繼續進行。

風險評鑑可使用數種已備妥的選項，以評估替代的概念，協助決定何者提供正面與負面風險的最佳平衡。

在設計與發展階段中，風險評鑑有助於：

- 確保系統風險為可忍受的。
- 設計改良過程。
- 成本有效性研究。

- 鑑別風險對後續的生命週期階段之衝擊。

於活動進行中，可使用風險評鑑來提供資訊，以協助發展正常與緊急狀況之程序。

6. 風險評鑑技術之選擇

6.1 一般

本節敘述風險評鑑技術可如何選擇。附錄列舉與進一步說明可用以執行風險評鑑或協助風險評鑑過程的工具與技術範圍。有時可能必需使用一種以上的評鑑方法。

6.2 技術之選擇

風險評鑑可以不同的深度與詳細程度，且使用範圍由簡單至複雜的一或多種方法進行。評鑑之形式與其輸出，須與作為建立前後環節的部分所制定之風險準則一致。

附錄A說明廣泛種類的風險評鑑技術間之概念關係，與設定風險情況中存在之因素，

並提供組織可如何選擇特定情況適宜的風險評鑑技術之說明範例。

一般而言，適合的技術須展現下列特性。

- 須為理由充分且適合於考慮的情況或組織。

處理之形式提供後果。

- 使用之方式須為可追溯、可重複及可查證者。

須針對關聯與適合性提出技術選擇之理由。

當由不同的研究整合後果時，使用的技術與輸出須對等。

一旦已作成實施風險評鑑之決策，且目標與範圍已界定，須依據諸如下列適用的因素選擇技術。

- 研究之目標。風險評鑑的目標會有差異性，與所使用的技術有關。例如，

此系統未受到差異性影響之部分，使用較不詳細的後果模式係可接受的。

- 決策者之需求。在某些情況中，需有高度的詳盡來做成良好決策，而其他則更一般性的瞭解即已足夠。
- 進行分析的風險之類型與範圍。
- 後果之潛在幅度。有關實施評鑑的深度之決策須反映後果最初的感知(雖然完成初步評估後，此可能必須予以修改)。
- 專家、人員及其他資源需求之程度。使用簡單的方法，做的妥善，可能較

粗略地做完極為複雜的程序，在符合評鑑的目標與範圍上，提供更佳的後果。通常，投入於評鑑的努力成果須與所分析的風險之可能等級一致。

- 資訊與資料之可取得性。某些技術較其餘者需要更多資訊與資料。
- 風險評鑑的修改/更新之需求。評鑑未來可能需予以修改/更新，而某些技術在此方面可能較其餘者更多之修改。
- 任何法令規章與契約要求。

各種因素影響風險評鑑方式的選擇，諸如資源之可取得性、備妥資料與資訊的

不確定性之本質與程度，及實施之複雜性(參照表A.2)。

6.3 資源之可取得性

可能影響風險評鑑技術選擇的資源與能力包括：

- 風險評鑑小組技能經驗之能量與能力。
- 組織內有關時間與其他資源之限制。
- 若需要外部資源時可取得之預算。

6.4 不確定性之本質與程度

不確定性之本質與程度要求對有關所考量的風險可取得資訊之品質、數量及完整性

的瞭解，此包括有關此風險充分的資訊範圍、其緣由與原因，以及目標達成可得到的後果。不確定性可源自不佳的資料品質或缺乏必要與可靠的資料。例如，資料蒐集方法可能改變、組織使用此方法的方式可能改變，或組織對於蒐集有關已鑑別風險之資料，可能完全未具備有效的蒐集方法。

不確定性亦可能原來已存在於組織的外部與內部前後環節中。所備妥之資料對於未來之預測並不經常提供可靠的基礎。對於獨特類型的風險，歷史資料可能無法取

，或可取得資料對不同的利害相關者可能得到不同的解讀。承辦風險評鑑者需瞭解此不確定性之類型與本質，並重視風險評鑑結果可靠度之含意。若有此類情況，須切記向決策者報告說明。

6.5 複雜性

風險本身可能係複雜的，例如，在複雜系統中需要對其風險跨越整個系統加以評鑑，

而非個別處理每一成分而忽略彼等之互動性。在其他情況中，處理單一風險可能牽涉其他部分，且可能衝擊其他活動。重要

在管理單一風險時，無法忍受的情況不在他處形成。瞭解組織的單一風險或風險組合之複雜性，對於選擇風險評鑑的適當方法或技術係極為重要的。

6.6 生命週期階段中風險評鑑之應用

許多活動、專案及產品可被考量具有生命週期，由起始的概念與定義開始經由實現至最終完結，此可能包括硬體的汰除與最終處理。

風險評鑑可應用於生命週期之所有階段，

且通常實施多次，各具不同的詳細程度，以協助在每一階段所需形成的決策。

生命週期階段具有不同的要求且需要不同的技術。例如，在概念與定義階段中，當一機會已予鑑別，可使用風險評鑑以決定是否繼續進行。

風險評鑑可使用數種已備妥的選項，以評估替代的概念，協助決定何者提供風險的最佳平衡。

在設計與發展階段中，風險評鑑有助於：

- 確保系統風險為可忍受的。
- 設計改良過程。

- 成本有效性研究。
- 鑑別風險對後續的生命週期階段之衝擊。

於活動進行中，可使用風險評鑑來提供資訊，以協助發展正常與緊急狀況之程序。

6.7 風險評鑑技術之類型

風險評鑑技術可以不同方式予以分類，以協助瞭解其相對優勢與弱點。為闡述目的，

附錄A聯結一些有潛力的技術及其分類。

每一項技術依據評鑑之本質進一步詳述於附錄B，提供在某些情況下其應用之指

附錄A
（參考）
風險評鑑技術之比較

A.1 技術類型

首先，分類如下列顯示此等技術如何應用於風險評鑑過程之每一步驟。

- 風險鑑別。
- 風險分析－後果分析。
- 風險分析－定性、半定量或定量機率估計。
- 風險分析－評鑑任何既有的控管之

有效性。

- 風險分析－風險等級估計。
- 風險評估。

對風險評鑑過程之每一步驟，方法的應用以極適用、適用或不適用敘述之(參照表A.1)。

A.2 影響風險評鑑技術選擇之因素

其次，依下列觀點描述方法之屬性。

- 問題與其分析所需方法的複雜性。
- 風險評鑑的不確定性之本質與程度，

依據可取得資料量與被要求何者來滿足目標而定。

- 依時間與專業水準、資料需求或成本之觀點，所需的資源之期間與範圍。
- 此方法是否可提供定量輸出。

可利用的風險評鑑方法類型之範例列於表A.2，其中每一方法依其屬性之觀點評定為高、中或低。

表A.1　風險評鑑使用工具之適用性

工具與技術	風險評鑑過程					
	風險鑑別	風險分析			風險評估	參照附錄
		後果	機率	風險等級		
腦力激盪	極適用	不適用	不適用	不適用	不適用	B 01
結構化或半結構化面談	極適用	不適用	不適用	不適用	不適用	B 02
德爾菲(Delphi)	極適用	不適用	不適用	不適用	不適用	B 03
查檢表	極適用	不適用	不適用	不適用	不適用	B 04
初期危害分析(PHA)	極適用	不適用	不適用	不適用	不適用	B 05
危害與可操作性研究(HAZOP)	極適用	極適用	適用	適用	適用	B 06
危害分析與關鍵管制點(HACCP)	極適用	極適用	不適用	不適用	極適用	B 07

表A.1　風險評鑑使用工具之適用性(續)

工具與技術	風險評鑑過程					
	風險鑑別	風險分析			風險評估	參照附錄
		後果	機率	風險等級		
環境風險評鑑	極適用	極適用	極適用	極適用	極適用	B 08
結構化之〝如果這樣會怎樣？〞(SWIFT)	極適用	極適用	極適用	極適用	極適用	B 09
情境分析	極適用	極適用	適用	適用	適用	B 10
企業衝擊分析(BIA)	適用	極適用	適用	適用	適用	B 11
根本原因分析(RCA)	不適用	極適用	極適用	極適用	極適用	B 12
失效模式與效應分析(FMEA)	極適用	極適用	極適用	極適用	極適用	B 13
失效(故障)樹分析(FTA)	適用	不適用	極適用	適用	適用	B 14

事件樹分析(ETA)	適用	極適用	適用	適用	不適用	B 15
因果分析	適用	極適用	極適用	適用	適用	B 16
原因與效應分析	極適用	極適用	不適用	不適用	不適用	B 17
保護層分析(LOPA)	適用	極適用	適用	適用	不適用	B 18
決策樹	不適用	極適用	極適用	適用	適用	B 19
人因可靠度分析	極適用	極適用	極適用	極適用	適用	B 20
蝴蝶結分析	不適用	適用	極適用	極適用	適用	B 21
可靠度中心維護(RCM)	極適用	極適用	極適用	極適用	極適用	B 22
潛行路徑分析(SCA)	適用	不適用	不適用	不適用	不適用	B 23
馬可夫(Markov)分析	適用	極適用	不適用	不適用	不適用	B 24

蒙地卡羅模擬	不適用	不適用	不適用	不適用	極適用	B 25
貝氏統計法(Bayesian statistics)與貝氏網路(Bayes Nets)	不適用	極適用	不適用	不適用	極適用	B 26
FN曲線	適用	極適用	極適用	適用	極適用	B 27
風險指數	適用	極適用	極適用	適用	極適用	B 28
後果/機率矩陣	極適用	極適用	極適用	極適用	適用	B 29
成本/效益分析(CBA)	適用	極適用	適用	適用	適用	B 30
多準則決策分析(MCDA)	適用	極適用	適用	極適用	適用	B 31

表A.2　風險評鑑工具選擇之屬性

典型的風險評鑑方法與技術	描述	影響因素之關聯性			可提供定量輸出
		資源與能力	不確定性之本質與程度	複雜性	
查詢方法					
查檢表	簡單的風險鑑別格式。提供需予以考量的典型不確定性之列表。使用者對照先前制定的一覽表、規章或標準。	低	低	低	否
初期危害分析	簡單的歸納分析方法，其目標為鑑別可能造成一特定活動、設施或系統傷害的危害與危害情況及事件。	低	高	中	否

支援方法					
結構化面談與腦力激盪	由一小組蒐集廣泛的想法並評估、排序之方式。腦力激盪可透過提示或一對一與一對多的面談技術予以激發。	低	低	低	否
德爾菲(Delphi)技術	綜合專家的意見之方式，可支援緣由與影響之鑑別，機率與後果估計及風險評估。為在專家間建立共識之合作技術。 涉及專家的獨立分析與表決。	中	中	中	否
SWIFT結構化之〝如果這樣會怎樣〞	驅使小組鑑別風險之系統。通常使用在促進研討會中。通常與風險分析與評估技術相連結。	中	中	任一	否

人因可靠度分析(HRA)	人因可靠度評鑑(HRA)，涉及人類對系統性能之影響，並可用以評估人為失誤對系統之影響。	中	中	中	是
情境分析					
根本原因分析(單一損失分析)	分析已產生的單一損失以瞭解造成的原因，以及此系統或過程可如何改進以避免未來發生此等損失。此分析應考量產生損失當時具備的控管，與可如何改進控管。	中	低	中	否
情境分析	透過經考量的現有與不同風險之想像或外插，假設每一此等情境皆可能發生，以鑑別出未來可能的情境。此可以正式或非正式的定性或定量方式進行。	中	高	中	否

毒性風險評鑑	危害予以鑑別與分析，以及特定標的可能暴露於危害之可能途徑亦予以鑑別。暴露程度之資訊與有關所規定的暴露程度造成的傷害本質之資訊經合併，以得到特定傷害會產生的機率之量測。	高	高	中	是
企業衝擊分析	提供主要的破壞風險可能如何影響組織的作業之分析，以及鑑別並量化管理所需的製程能力分析。	中	中	中	否

表A.2　風險評鑑工具選擇之屬性(續)

典型的風險評鑑方法與技術	描述	影響因素之關聯性			可提供定量輸出
		資源與能力	不確定性之本質與程度	複雜性	
失效(故障)樹分析(FTA)	由最不期望的事件(頂端事件)開始，並決定所有可能發生的方式之技術。以有條理的樹狀圖圖示呈現之。一旦失效(故障)樹經予發展，須考量降低或消除潛在原因/緣由之方式。	高	高	中	是
事件樹分析	使用歸納性的推論，將不同的起始事件之機率轉化為可能後果。	中	中	中	是
因果分析	失效(故障)樹與事件樹分析之組合，允許納入時間的延遲。起始事件之原因與後果均予以考量。	高	中	高	是

原因與效應分析	一效應可能具有一些可歸類為不同分類的促成因素。促成因素通常透過腦力激盪並以樹狀構造或魚骨圖呈現予以鑑別出。	低	低	中	否
功能分析					
失效模式與效應分析(FMEA)以及失效模式與效應及關鍵性分析(FMECA)	失效模式與效應分析(FMEA)係鑑別失效模式與機制及其效應之技術。 有數種類型的FMEA：設計(或產品)FMEA用於零件與產品，系統FMEA用於系統，過程FMEA用於製造與組裝過程，服務FMEA及軟體FMEA。 FMEA可跟隨以定性、半定量或定量方式界定每一失效模式的顯著性之關鍵性分析(FMECA)。關鍵性分析可依據失效模式將造成系統失效的機率，或與失效模式相伴而生的風險等級，或風險優先序號。	中	中	中	是

可靠度為中心之維護	鑑別某項政策的方法，此政策須予以實施以管理各種失效，使有效率與有效果地達成所有型式設備作業所要求之安全、可使用性及經濟性。	中	中	中	是
潛行分析（潛行路徑分析）	鑑別設計失誤之方法。潛行狀況為隱藏的硬體、軟體或整體狀況，可能造成不期望的事件發生或可能抑制期望的事件，且並非因零件失效所造成。此等狀況的特性為其隨機本質，及在最嚴格的標準化系統測試中逃避偵測之能力。潛行狀況可能造成不當的操作、系統可用性之損耗、計畫延遲、或甚至人員的死亡或受傷。	中	中	中	否

表A.2　風險評鑑工具選擇之屬性(續)

典型的風險評鑑方法與技術	描述	影響因素之關聯性			可提供定量輸出
		資源與能力	不確定性之本質與程度	複雜性	
危害與可操作性研究(HAZOP)	風險鑑別之一般過程，用以界定與預期或希望的性能的可能偏差。使用導引詞為基礎的系統。 使偏差之關鍵性得以評鑑。	中	高	高	否
危害分析與關鍵管制點(HACCP)	系統化、預應性及預防性系統，透過量測與監測要求在界定限值內的特定特性，用以確保產品品質，過程之可靠性與安全。	中	中	中	否

控管評鑑					
保護層分析(LOPA)	(亦可稱為障礙分析)使得以評估控管與其有效性。	中	中	中	是
蝴蝶結分析	描述與分析風險由危險形成後果之途徑及審查其控管的簡單圖示方法。可視為失效(故障)樹分析事件之導因(以蝴蝶結之結表示)，與事件樹分析後果的邏輯組合。	中	高	中	是
統計方法					
馬可夫(Markov)分析	馬可夫分析有時稱為狀態空間分析，通常使用於可存在於多種狀態，包括各種等級狀態的可修復複雜系統之分析。	高	低	高	是

蒙地卡羅分析	蒙地卡羅模擬用以建立一些輸入的系統內之變異導致的系統總變異，每一輸入具有界定的分配，且輸入透過界定的關係關聯至輸出。此分析可用於各種輸入可數學界定的特定模式。輸入可依據其意圖表示的不確定性之本質，以各種分配為基礎。對於風險評鑑，一般使用三角分配或β分配。	高	低	高	是
貝氏分析	利用先前分配數據評估後果的機率之統計程序。貝氏分析依據先前分配之準確度推導出精確的結果。貝氏相信在不同領域中聯網模式之原因與效應，透過擷取變數輸入之機率學關係，導出結果。	高	低	高	是

附錄B

（參考）

風險評鑑技術

B.1　腦力激盪

B.1.1 一般

腦力激盪含有激發與鼓勵一組知識豐富的人員之間自由交流的對話，以鑑別可能的失效模式與相關的危害、風險、決策之準則及/

或處理之選項。〝腦力激盪〞一詞通常不受拘束地用以泛指任何型式的小組討論。然而真正的腦力激盪牽涉到嘗試確使人員的想像力受到小組中其他人員的思維與陳述觸發之特殊技術。

有效之引導在此技術中係極重要的，且包括在開始時激發討論，周期地驅使小組進入其他相關領域，並擷取由此討論中產生的議題(通常極為熱烈地)。

B.1.2 應用

腦力激盪可與下述之其他風險評鑑方法一併使用，或可單獨進行作為風險管理過程之任何階段與系統的生命週期之任何階段激勵想像的思維之一項技術。其可應用於議題已鑑別的高階討論會，更詳盡地審查會或對特定問題之細節層面。

腦力激盪特別強調想像力。因此，當鑑別新技術的風險時，於缺乏資料之場合或對問題需有創新的解決方案時特別有效。

B.1.3 輸入

一組人員具備對接受評鑑的組織、系統、過程或應用之知識。

B.1.4 過程

腦力激盪可為正式或非正式。正式的腦力激盪更為結構化，與會者事先準備且該會議具有界定的目的與成果，事先設定評估構思的方式。非正式的腦力激盪則較低結構化且通常更傾向視情況個案處理。

在正式的過程中：

- 引言者準備思維之提示，且在會議之前適宜地啟發該前後環節。
- 會議之目標已界定且規則已說明。
- 引言者起動思維的延續，且每一人發掘想法以鑑別儘可能多的議題。在此時，不討論有關事項是否須列入清單或特定陳述之含意，因其易於抑制自由交流之思維。所

有輸入均予接受且無遭受挑剔，小組進展迅速以使想法啟發旁側的思維。

• 當單一方向之思維耗盡或討論偏離太遠時，

引言者可啟發人員新的思路。無論如何，蒐集的想法儘可能多，以供後繼之分析。

B.1.5 輸出

輸出依風險管理過程實施之階段而定，例如在鑑別階段時，輸出可能係一份列有風險

B.1.6 優勢與限制

腦力激盪的優勢包括：

- 激勵想像力有助於鑑別新風險與創新的解決方案。
- 含有主要的利害相關者且因而有助於整體的溝通。
- 相對較快速且易於發起。

限制包括：

- 與會者可能缺乏技能與知識以成為有效的貢獻者。
- 由於其相對地低度結構化，難以展現對此過程已涵蓋全部事項，例如所有潛在的風險均予以鑑別。
- 可能出現特殊的群組動力，當某些人員準備陳述有價值的想法時但保持沉默，其他人員主導此討論。此可藉由電腦腦

力激盪，使用閒聊式公開討論或規劃的小組技術予以克服。電腦腦力激盪可設定為不記名者，因此可避免可能妨礙自由交流的想法之個人與政治議題。在名義上的小組技術中，將想法以不具名方式提交會議主持人，然後再由小組討論。

B.2　結構化或半結構化面談

B.2.1 一般

在結構化的面談中，個人受訪者被詢問一組備妥的問題提示表單，鼓勵該受訪者由

不同之觀點審視情況，然後再由此觀點鑑別風險。半結構化面談相同，但允許更自由地對話以探究所產生之議題。

B.2.2 應用

如難以聚集人員進行腦力激盪會議，或因情況或所涉人員不適宜在小組中自由交流討論，則可使用結構化與半結構化面談為。其最常用以鑑別風險或評鑑作為風險分析的一部分之既有控管之有效性。其可在專案或過程之任何階段實施。其為提供利害相關者輸入至風險評鑑之一方式。

B.2.3 輸入

輸入包括：

- 面談目標的清楚界定。
- 由相關的利害相關者選出之受訪者名單。
- 一組已備妥的問題。

B.2.4 過程

建立相關的問題組以引導面談者。問題儘可能須為開放的，須為簡單的，以受訪者

適宜的語言並僅涵蓋一項議題。亦備妥更進一步探究以尋求闡明之可能的問題。

然後將問題提出給接受面談的人員。當尋求合作時，問題須為開放的。須小心不致〝誘導〞受訪者。

回應須具有彈性性地予以考量，以提供探究受訪者可能希望進入的領域之機會。

B.2.5 輸出

輸出為利害相關者對此次面談主題有關的議題之意見。

B.2.6優勢與限制

結構化面談之優勢如下列：

- 結構化面談使人員有時間考量有關一項議題的思維。
- 一對一溝通可更深入考量議題。
- 結構化面談較使用相對小型的小組之腦力

激盪，可涉及更多數的利害相關者。

限制如下列：

- 對於引言者以此方式取得多數之意見係耗時的。
- 容許偏差且並未透過小組討論移除。
- 想像力的啟發為腦力激盪之特徵，可能無法達成。

B.3　德爾菲(Delphi)技術

B.3.1 一般

德爾菲(Delphi)技術係由一組專家取得可信賴意見的共識之程序。雖然此用語現在經常廣泛地用以泛指任何形式的腦力激盪，德爾菲(Delphi)技術主要之特徵，如同原始明確陳述者，係專家在過程進行中，當接收到其他專家的意見時，個別與不具名地表達其意見。

B.3.2 應用

德爾菲(Delphi)技術可應用於當專家的

需達成共識時，風險管理過程之任何階段或系統生命週期之任何階段。

B.3.3 輸入

需何項共識的一個選項集合。

B.3.4 過程

使用半結構化的問卷詢問一組專家。專家們互不相遇，因此其意見為獨立的。

程序依下列：

- 組成一小組以執行與監測此德爾菲(Delphi)過程。
- 選擇一組專家(可為一或多個專門委員會)。
- 制定第一回合問卷。
- 測試此問卷。
- 個別寄送問卷至專家小組成員。
- 分析並彙總第一回合回覆之資訊及再寄發至專家小組成員。

- 專家小組成員回覆，並重複此過程直至達成共識。

B.3.5 輸出

對進行中的事務彙整朝向共識

B.3.6 優勢與限制

優勢包括：

- 因意見為不具名，可能表達更多非主流的意見。

- 所有意見同樣重要，避免佔優勢人士把持問題。
- 呈現成果之擔當者精神。
- 人員不需邀約在同一時間於同一地點聚集。

限制包括：

- 勞動密集且耗時。
- 與會者本身需能以書面清楚表達。

B.4 查檢表

B.4.1 一般

查檢表為依先前風險評鑑結果或依過去失效的結果之經驗，發展出的危害、風險或控管失效一覽表。

B.4.2 應用

查檢表可用以鑑別危害與風險，或評鑑控管的有效性。其可應用於產品、過程或服務的生命週期任何階段。其可能作為其他

風險評鑑技術之一部分，但在應用於已實施更具想像力的技術鑑別新問題之後，查核所涵蓋之每件事時最有效。

B.4.3 輸入

有關此議題之前的資訊與專家意見，使相關與喜好的確認查檢表可予以選擇或制定。

B.4.4 過程

程序如下列：

• 已選定適切涵蓋範圍之查檢表。為此目的需小心選擇查檢表，例如使用標準控管之查檢表並不足以鑑別新的危害或風險。

• 人員或小組依查表之步驟，逐條審視過程或系統之每一要項，並審查查檢表上之項目是否仍適用現況。

B.4.5 輸出

輸出依據風險管理過程實施之階段而定。例如輸出可能為不適切控管之清單或風險清單。

B.4.6 優勢與限制

查檢表之優勢包括：

- 可由非專家使用。
- 當經適當設計，其們將廣泛範圍的專家意見結合至易於使用的系統中。
- 其們可協助確保通案問題不致遺忘。

限制包括：

- 其們傾向抑制風險鑑別之想像力。

- 其們強調〝熟知已知的(known knowns)〞，而非〝熟知未知的(known unknowns)〞或〝不知未知的(unknown unknowns)〞。
- 其們鼓勵〝在格子裡打勾(tick the box)〞式的行為。
- 其們傾向以觀察為基礎的，因此漏失事先未被察覺之問題。

B.5　初期危害分析(PHA)

B.5.1 一般

PHA為一簡單、歸納的分析方法，其目標係鑑別特定的活動、設施或系統可造成傷害的危害與危害情況及事件。

B.5.2 應用

PHA為最通常在擬訂專案之早期，當具有些許設計細節或作業程序之資訊時施行之，且通常可為預備的，供進一步研究或提供

系統設計規範之資訊。當分析現有系統優先性的危害與風險俾以進一步分析時，或當情況妨礙使用更廣泛的技術時，亦可為有用的。

B.5.3 輸入

輸入包括：

- 有關欲評鑑的系統之資訊。
- 系統設計可取得與相關的此等系統設計細節。

B.5.4 過程

藉由考量如下列之特性所形成之危害與一般危害情況及風險之清單。

- 使用或製造出來的材料及其反應性。
- 使用的設備。
- 作業環境。
- 配置。
- 系統零組件間的介面等。方式呈現之。

可對不期望的事件與其機率的後果作定性分析以鑑別風險，供進一步評鑑。

在設計、建構及測試階段中PHA須予以更新，以偵測任何新危害，且若必要時進行修正。獲得的結果可以諸如表格與樹狀圖等不同方式呈現之。

B.5.5 輸出

輸出包括：

- 一份危害與風險的清單。

- 以接受、建議之控管、設計規範或更詳細評鑑之要求等格式作成建議事項。

B.5.6 優勢與限制

優勢包括：

- 足可在僅具有限資訊時使用。
- PHA使風險在系統生命週期極早期時即予考量。

限制包括：

・PHA僅提供初期資訊，並非完整的，亦不提供有關風險與其如何可最佳地予以預防之詳細資訊。

B.6 危害與可操作性研究(HAZOP)

B.6.1 一般

HAZOP係危害(HAZard)與可操作性(OPerability)研究之頭字語，係對經規劃的或目前的產品、過程、程序或系統之結構化與系統化檢查。HAZOP係一種鑑別人員

、設備、環境及/或組織的目標之風險的技術。惟亦期望研究小組在可能時提供處理此風險之解決方案。

HAZOP過程為以引導詞之使用為基礎的一項定性技術，此引導詞詢問在設計、過程、程序或系統的每一步驟，意圖或作業狀況何者或如何可能無法達成引導詞。HAZOP通常以多學科的小組之方式，在一系列的會議中施行。

HAZOP與失效模式與效應分析(FMEA)類似，均為鑑別過程、系統或程序的失效模式、

其原因及後果。與其相異之處為小組考量不期望的後果相對於預期的結果與狀況之偏差，並回頭研究可能引起失效之模式，然而FMEA係在開始時即鑑別失效模式。

B.6.2 應用

HAZOP技術最初發展用以分析化學製程系統，經擴展至其他型式的系統與複雜性作業。此等包括機械與電子系統、程序及軟體系統，甚且至組織的變動與法律合約設計與審查。

HAZOP過程可處理因設計、零件、所規劃的程序及人類行為之缺陷，而產生的所有形式的設計目的之偏差。

HAZOP廣泛使用於軟體設計審查，當應用於管制安全關鍵性裝置與電腦系統時，可能熟知為CHAZOP(管制危害與可操作性分析或電腦危害與可操作性分析)。

HAZOP研究通常在細部設計階段，預期的過程之完整構圖已備妥，但設計之變更仍為可行時進行，然而，其可以分階段的方式執行，每一階段具有不同的引導詞作為

細節之設計發展。HAZOP研究亦可在作業進行中執行，但在該階段所需之變動可能耗費大。

B.6.3 輸入

HAZOP研究的主要輸入包括有關欲審查的此系統、過程或程序目前之資訊，與該設計的意圖與性能規範。輸入可能包括：繪圖、規格表單、流程表單、過程管制與邏輯圖、配置圖、操作與維護程序及緊急應變程序。對於非屬硬體有關的HAZOP，輸入

可為敘述研究中的系統或程序功能與要素之任何文件。例如，輸入可為組織圖與角色說明，合約草案或甚至為程序書草案。

B.6.4 過程

HAZOP採取欲研究的過程、程序或系統之〝設計〞與規範，並審查其每一部分，以找出與預期的性能可能產生的偏差為何、潛在的原因為何，以及偏差可能的後果為何。此可藉使用適當的引導詞，透過系統化地檢查每一部分的系統、過程或程序將如何回應關鍵參數的變化予以達成。引導

詞可為特定的系統、過程或程序量身定製的，或可使用涵蓋所有偏差類型的一般字眼。表B.1提供一般使用的技術系統引導詞之範例。可使用類似的引導詞如〝太早〞、〝太遲〞、〝太多〞、〝太少〞、〝太長〞、〝太短〞、〝錯誤方向〞、〝錯誤對象〞〝錯誤行動〞等用以鑑別人為之錯誤模式。

HAZOP研究之正常步驟包括：

- 提名一位負有必要責任與職權之人員來

執行HAZOP研究，並確保由此研究產生的任何行動均已完成。

- 界定此研究之目標與範圍。
- 建立此研究的一組關鍵字或引導詞。
- 界定HAZOP研究小組，此小組通常包括多種專門學科，且須包括具有適宜技術專業的設計與作業人員，以評估與預期或目前設計的偏差之效應。建議該小組包括不直接涉及進行審查的設計或系

過程或程序之人員。

- 蒐集所需的文件。

在研究小組的促進研討會中：

- 將系統、過程或程序區分為較小要項或次系統或次過程或次要項，以進行實質審查。
- 協議每一次系統、次過程或次要項之設計目的，而後對此次系統或要項之每一

項目，逐項應用引導詞來假定將具有不期望結果之可能的偏差。

- 如鑑別出不期望的結果，協議每一案例的原因與後果，並建議其可如何予以處理，以預防其發生，或當發生時減輕該後果。
- 文件化此項處理所鑑別的風險之特定措施的討論與協議。

表B.1　可能的HAZOP引導詞範例

用語	定義
無或非	無任何部分達成預期的結果，或預期的狀況不存在
更多(更高)	輸出或作業狀況中定量的增加
更少(更低)	定量的減少
不僅...又	定量的增加(如額外的材料)
部分的	定量的減少(如混合物中僅有一或兩種成分)
反轉/逆向	相反的(如逆流)
(與...)不同的	無任何部分達成預期，完全不同的事件發生(如流動或錯誤材料)
相容性	材料、環境

引導詞應用至諸如下列參數	
	材料或過程之物理性質
	物理狀況如溫度、速度
	系統或設計的一組成之特定意圖(如資訊傳遞)
	操作的層面

B.6.5 輸出

記錄逐一審查點的項目之HAZOP會議紀錄。此包括：使用的引導詞、偏差、可能的原因、處理所鑑別問題之措施及此措施負責人員

員。對無法予以矯正的任何偏差，則此偏差之風險須予以評鑑。

B.6.6 優勢與限制

HAZOP分析提供下列益處。

- 提供系統化與完全地檢查系統、過程或程序之方式。
- 包含多種專門學科的小組，包括具有實在的作業經驗之人員及可能必須執行處理措施的人員。
- 產生解決方案與風險處理措施。

- 適用於廣泛範圍的系統、過程及程序。
- 使清晰考量人為錯誤之原因與後果。
- 建立過程的書面紀錄，可用以展現應有的嚴謹度。

限制包括：

- 詳細的分析可能非常耗時，且因此為昂貴的。
- 詳細的分析需要高水準的文件化或系統/過程與程序規範。
- 與其挑戰根本假設(雖然，此可以分階段之方式予以減輕)，不如可著重於尋

找詳細的解決方案。

- 討論可著重於設計之詳細議題，而非廣泛或外部議題。
- 受到設計(草案)與設計意圖，及賦予小組的範圍與目標之限制。
- 過程極依賴設計者之專業技術，其可能發現難以充分客觀地在其設計中尋找問題。

B.6.7 參考文件

IEC 61882 Hazard and operability studies (HAZOP studies) - Application

guide

B.7危害分析與關鍵管制點(HACCP)

B.7.1一般

危害分析與關鍵管制點(HACCP)提供鑑別危害，並在過程的所有相關部分恰當地置放管制之架構，以對此危害防護並維持產品品質之可靠度與安全。HACCP目標為確保風險與其經由終端產品的檢驗，不如透過整體過程的管制予以降低。

B.7.2 應用

HACCP係為確保美國航空太空總署(NASA)太空計畫的食物品質而發展出。現今由組織使用在食物鏈中任何處之操作，以管制來自於食物的物理、化學或生物污染之風險。其亦已擴展使用於藥品及醫療器材的製造，鑑別可影響產品品質的事物之原則，以及界定過程中關鍵性參數可予以監測與管制危害之定點，可推廣至其他技術系統。

B.7.3 輸入

HACCP由基本的流程圖或過程圖，以及有關可能影響輸出產品或過程品質、安全或可靠度的危害之資訊開始。有關危害與其風險，以及其可予以控管之方式等資訊，為HACCP之輸入。

B.7.4 過程

HACCP包含下列七項原則。

- 鑑別此等危害之危害與預防措施。
- 決定過程中可控管或去除危害之點(關鍵管制點或CCPs)。

- 建立控管此危害所需的臨界界限，即每一關鍵管制點須在特定參數範圍內作業以確保危害受到控管。
- 在界定之時間間隔監測每一關鍵管制點之臨界界限。
- 若過程落於所建立的界限之外，則建立矯正措施。
- 建立查證程序。
- 實施每一步驟之紀錄維持與文件化程序。

B.7.5 輸出

文件化的紀錄包含危害分析作業計畫表與HACCP計畫。

危害分析作業計畫表列出過程之每一步驟：

- 在此步驟中可能引入、控管或惡化的危害。
- 此危害是否存有顯著的風險(依據經驗、資料及技術文獻組合的後果與機率之考量)。
- 此顯著性之正當判斷。
- 每一項危害可能的預防措施。
- 監測或控管措施是否可在此步驟實施(

即其是否為關鍵管制點？）。

HACCP計畫描述為確保步驟的設計、產品、過程或程序之控管應遵守的程序。此計畫包括所有關鍵管制點與下列每一關鍵管制點的：

- 預防措施之關鍵界限。
- 監測與持續控管活動(包括何種、如何及何時進行監測，以及由何人監測)。
- 若偵測到對關鍵界限之偏差，所需之矯正措施。
- 查證與維持紀錄之活動。

B.7.6 優勢與限制

優勢包括：

- 結構化的過程提供品質管制以及鑑別與降低風險之文件化證據。
- 著重於過程中如何與何處可予以預防危害，並控管風險之實用性。
- 與其依賴最終產品檢查，不如整個過程更佳的風險控管。

鑑別經由人為導致的危害，以及在導致點或隨後之發展點如何予以控管之能力。

限制包括：

- HACCP要求鑑別危害、界定存在的風險、瞭解作為過程的輸入之重要性。界定適宜之控管。此等要求係為規定HACCP中之關鍵管制點與控管參數，且可能需與其他工具結合以達成。
- 當控管參數超過界定界限始採取行動，可能遺漏在統計上顯著而須採取措施之控管參數漸變狀況。

B.7.7 參考文件

CNS 22000食品安全管理系統－食品供應鏈

中組織之要求

B.8　毒性評鑑

B.8.1 一般

此處使用環境風險評鑑以涵蓋在評鑑植物、動物及人類暴露在某一範圍的環境危害中時應遵循的過程。風險管理提及包括風險評估與風險處理的決策過程。

此方法涉及分析傷害之危害或緣由，及其如何影響標的群體，以及此危害可能侵犯易受感染的標的群體之途徑。然後結合此資訊以提出可能的傷害範圍與本質之估計

B.8.2 應用

此過程用以評鑑植物、動物及人類暴露於諸如化學品、微生物或其他物種的危害所導致的風險。

此方法之考量面，諸如途徑分析，調查標的物可能暴露於風險緣由的不同路徑，可予以適應並橫跨使用於除人體健康與環境外，極廣泛範圍之不同風險領域，且對鑑別降低風險的處理措施有所助益。

B.8.3 輸入

此方法需要有關危害的本質與特性之資料

、標的群體(或群體)之易受感染性，以及此兩者相互作用之方式。此資料通常依據可能為實驗室基礎或流行病學的研究。

B.8.4 過程

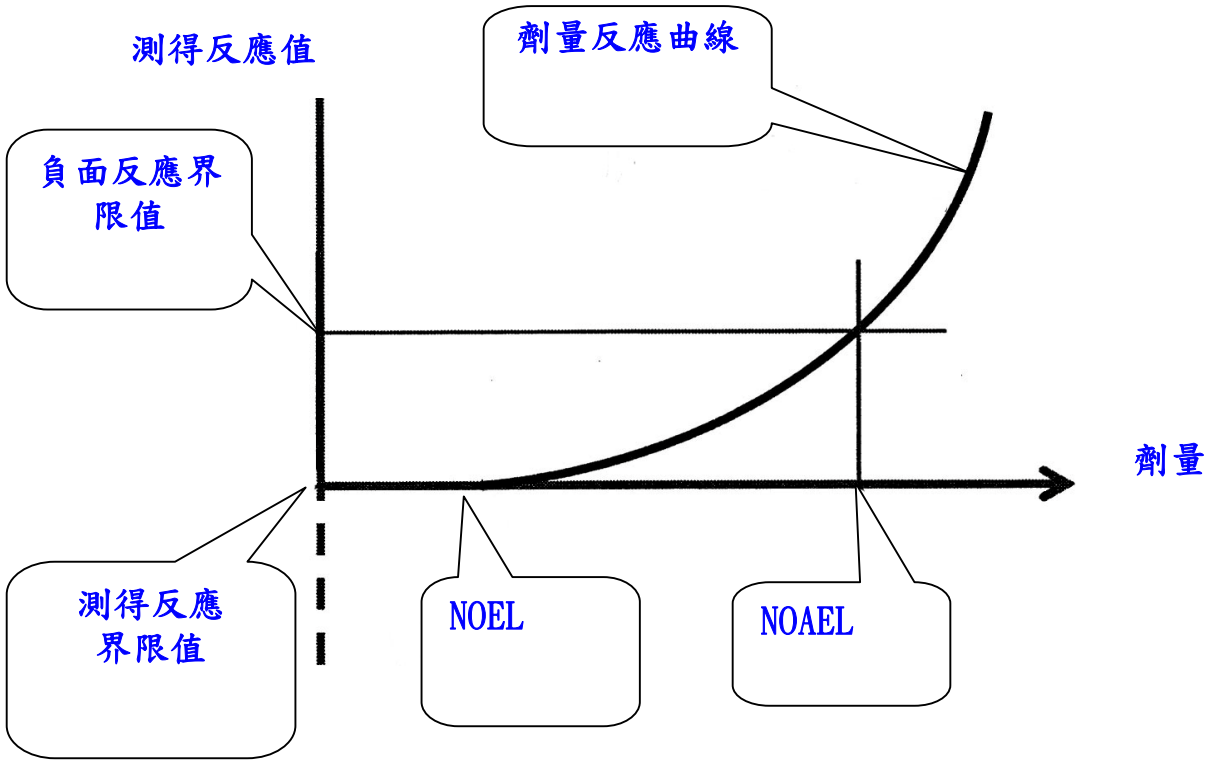
此程序如下：

(a)問題之系統陳述—此包括透過界定標的群體的範圍與關切的危害類型，設定評鑑之範圍。

(b)危害鑑別—此涉及鑑別研究範圍內之危害，對標的群體所有可能的傷害緣由。危害鑑別通常仰賴專家的知識與文獻之

參考。

(c)危害分析—此涉及瞭解危害的本質及其如何與標的相互作用。例如，當考量人類暴露於化學效應時，危害可能包括急性與慢性的毒性、破壞DNA之可能性，或導致癌症或生育缺陷之可能性。對每一危害效應，此效應之量(反應量)與標的暴露之危害量(劑量)相比較，且當可能時，測定此效應產生的機制。註記無明顯藥效劑量(NOEL)與無明顯藥害劑量(NOAEL)之水準。此等值有時作為風險接受度之準則。



圖B.1　劑量反應曲線

對於化學暴露，測試結果用以產生如圖B.1概略圖所示之劑量反應曲線。此通常由對動物或諸如培養組織或細胞的實驗系統所產生。諸如微生物或引進的物種等其他危害之效應。

，可由現場數據與流行病學的研究測定出。疾病或有害生物與標的物相互作用之本質可測定出，且由特殊暴露於危害的特殊傷害程度之機率可估算出。

(d)暴露分析－此步驟檢驗危害物質或其殘留物，可能如何達到可感染的標的群體，與其劑量為何。其通常包含途徑分析，考慮危害可能產生的不同路徑、可能阻止其侵犯標的物之障礙，以及可能影響暴露程度之因素。例如，在考量化學噴灑劑的風險時，暴露分析將考量化學品已噴灑量為何、以何種方式以及在何種狀況

、是否有人類或動物直接暴露、可能殘留於植物生命期之量為何、殺蟲劑深入土壤之環境命運、是否其可累積於動物體內，或其是否進入地下水。在生物安全性中，途徑分析可能考量進入國境之任何有害生物可能如何進入環境中，成形並散布。

(e)風險特性化－在此步驟中，將危害分析與暴露分析之資訊合併估算由所有途徑的效應合併時其特定後果之機率。如具有極多數危害或途徑，可進行初始篩選，且對較高風險情境進行詳細的危害與暴露分析及風險特性化。

B.8.5 輸出

輸出通常係在考量的前後環節下，特定標的暴露於特定危害的風險等級指標。風險可以定量、半定量或定性表示之。例如，癌症風險通常以人員特定暴露於污染下，歷經特定期間將產生癌症的機率之定量方式表示，半定量分析可用以導出一特定污染物或有害生物的風險指數，而定性輸出可為風險等級(如高、中、低)，或可能效應的實際數據之描述。

B.8.6 優勢與限制

此分析之優勢為關於問題之本質與增進風險的因素提供極詳盡的瞭解。

途徑分析通常對所有的風險領域為有用的工具，且得以鑑別可能如何與在何處改進控管或導入新的控管。

然而，其確實所需有的良好資料，通常無法取得，或其具有相關的高度不確定。例如，由動物暴露於高度危害所產生的劑量反應曲線，須予以外插以估算極低量污染對人類之效應，而達成方式有多種模式。如標的係環境而非人類，且危害並非化學品，則直接與研究的特殊狀況相關之資料

可能有限。

B.9 結構化之〝如果這樣會怎樣〞技術(SWIFT, Structured "What-if" Technique)

B.9.1 一般

結構化之〝如果這樣會怎樣〞技術(SWIFT)最初發展作為HAZOP之較簡易的替代技術。其係利用一系列〝提示〞詞彙或片語的系統化、以小組為基礎之研究，由引言者在研討會中使用以激勵與會者鑑別風險。引言者與小組使用標準的〝如果

這樣會怎樣〞型式詞句結合提示，研究一系統、工廠項目、組織或程序將如何受到該等正常作業與行為的偏差之影響。SWIFT通常較常應用於系統層面，但比HAZOP具較低的詳細程度。

B.9.2 應用

SWIFT最初設計作為化學與石化廠危害研究，此技術現已廣泛應用於一般系統、工廠項目、程序、組織。尤其是，用以檢驗變更的後果，及因而改變或造成新的風險。

B.9.3 輸入

在研究開始進行之前，系統、程序、工廠項目及/或變動必須小心界定。透過面談與透過文件、計畫與圖樣的研究，引言者建立外部與內部前後環節，通常，研究的項目、情況或系統區分為節點或主要要項以促進此分析過程，但在HAZOP之界定層面係甚少出現的。

另一項重要的輸入為研究小組表現的專業知識與經驗，其須予以小心挑選。所有利害相關者若可能時，須具有相似項目、系統、變更或情況經驗者共同出席。

B.9.4 過程

一般過程如下。

(a)研究開始進行之前，引言者準備適合的提示詞彙或片語列表，可依據標準組或建立者，使得以全面性審查危害或風險。

(b)在研討會中，外部與內部前後環節之項目、系統、變更或情況及研究範圍，經討論與協議。

(c)引言者要求與會者提出並討論。

— 已知的風險與危害。

— 先前的經驗與事故。

— 已知與既存的控管與安全保障。
— 法規要求與限制。

(d)使用〝如果這樣會怎樣〞詞句與提示字眼或主題建立問題以促進討論，使用的〝如果這樣會怎樣〞之詞句有〝如果…怎麼辦？〞、〝如果…將產生怎樣？〞、〝某人或某事可否…〞、〝任何人或任何事是否曾經…〞。此目的為激勵研究小組發掘可能的情境、其原因與後果及衝擊。

(e)風險予以總結且小組考量所具備的控管。

(f)風險、其原因、後果及預期的控管之描述經小組確認並記錄之。

(g)小組考量此控管是否適切與有效，並同意風險控管有效性之說明。若不盡滿意，小組進一步考量界定風險處理工作與可能的控管。

(h)在此討論中，提出進一步〝如果這樣會怎樣〞之問題以鑑別進一步的風險。

(i)引言者使用提示列表以監督此討論，並提出額外的議題與情境提供小組討論。

(j)通常使用定性或半定量方法來依優先性排序所建立的措施。此項風險評鑑通常考量既有的控管及其有效性來執行。

B.9.5 輸出

輸出包括一個風險排序的措施或工作之風險登錄冊。此等措施可成為未來風險處理計畫的基準。

B.9.6 優勢與限制

SWIFT之優勢為：

- 廣泛適用於所有形式的實體工廠或系統、情況或狀況、組織或活動。

- 小組僅需少量的準備。
- 相對迅速，且主要危害與風險在研討會議中可快速成為顯而易見。
- 此研究為〝系統導向〞，且容許與會者非但檢查組件失效所引發的結果，更可檢查系統對偏差之反應。
- 可用以鑑別過程與系統改進的機會，且通常可用以鑑別引導與增進其成功機率之措施。
- 負責目前控管與進一步風險處理措施的當責人員參與討論會，強化其責任。
- 僅需少許之努力即可建立風險登錄與風

險處理計畫。

- 雖然經常使用定性或半定量方式風險分級進行風險評鑑，並藉以排定對所產生的行動項目的關注優先順序，SWIFT可用以鑑別風險與危害，並更進一步將之納入定量研究之用。

SWIFT之限制為：

- 需要有經驗與有能力的引言者方可產生效能。
- 需要細心準備以使研討會小組之時間不致浪費。
- 若研討會小組並不具有廣泛足夠的經驗

基礎，或若提示系統不夠全面性，則某些風險或危害可能無法鑑別出來。

• 應用此一技術於高層次課題時，可能無法揭露複雜地、細節性或相互關聯的原因。

B.10 情境分析

B.10.1 一般

所謂情境分析係對未來的可能發展，發展出其敘述模式。情境分析可透過考量未來的可能轉換及發掘其連帶影響，以鑑別風險。可以使用情境組合以反應，(例如)〝最佳狀況〞、〝最壞狀況〞及〝預期狀況

〞分析每一情境的可能後果及其機率，以之作為分析風險時的一種敏感度分析形式。

情境分析之能力為藉由考量過去50年間科技、消費者喜好、社會見解等之主要轉變闡述之。情境分析無法預測此等改變之機率，但可考量結果並協助組織發展優勢與所需的恢復力，以適應可預見之變化。

B.10.2 應用

情境分析除考量目前的活動外，可用以協助作成政策性決策並規劃未來策略。其可扮演所有風險評鑑的三項組成之一部分。

對於鑑別與分析，可使用情境組反應，例如最佳狀況、最壞狀況及預期狀況來鑑別在特定狀況下何者可能發生，並分析每一情境的潛在結果及其機率。

情境分析可用以分析威脅與機會兩者可能如何發展，並可用於同時具有短期與長期時間背景的所有類型風險。依短期時間背景與良好資料，可能的情境可由目前狀況延伸得知，對於長期的時間背景或微弱資料，情境分析偏向於想像式，並可能需視為未來分析。

當共同體或組織的空間、時間及群體內

之正面結果與負面結果間，有強烈的分布差異時，情境分析可為有效的。

B.10.3 輸入

情境分析不可或缺者為一小組人員，其間具備相關變化的本質之瞭解(例如科技可能的進步)，且想像思索未來不必要由過去延伸。取得有關正在發生的變化之文獻與資料亦相當有用。

B.10.4 過程

情境分析之結構可有非正式或正式二種。建立小組與相關的溝通管道後，並界定問題之前後環節與考量的議題後，下一步

驟為鑑別可能產生的變化之本質。此將需深入探討主要的趨勢變化與其可能發生的時間點，以及有關未來的想像思維。

考量的變化可包括：

- 外部變化(如科技之變化)。
- 不久的未來需作成的決策，但其可具有各種結果。
- 利害相關者需求及其可能如何變化。
- 總體環境(法規、人口統計學等)內之變化。其中有些可能無法避免，而有些則仍不確定。

有時，變化可歸因於另一風險所引致之

後果。例如，氣候變遷之風險係來自於消費者有關食物里程之變化，此將影響何種食物可外銷獲利，以及何種食物可在當地栽植。

局部與總體因素或趨勢現在可列出並分級為(1)重要(2)不確定，特別留意最重要與最不確定之因素。關鍵因素或趨勢對應地標示，以顯示可發展情境之區域。

提出一系列的情境，每一情境專注於某個參數中的合理變化。

然後書寫每一情境之〝情節〞，告訴您如何可能由目前位置邁向主題情境，此情節

可包括增值情境的合理細節。
然後此情境可用以測試或評估原始的問題。測試考量任何顯著但可預測之因素(如使用典型)，且在其後發掘在新情境中此政策(活動)〝成功〞情況如何，並依據模式之假設使用〝如果這樣會怎樣〞之問題〝預測試〞結果。
當問題或提議針對每一情境予以評估後，可能明顯顯示其需予以修正，以使其更穩健或較少風險。其亦可能鑑別可顯示變化何時產生的某些領先指標。監測與回應領先指標可提供變動既有的規劃策略之機會

。

由於情境僅界定可能的未來〝片斷〞，重要的是確定考量特定結果(情境)產生之狀況、最壞狀況及預期狀況情境時，須進行一些嘗試以認定或表示每一情境發生的機率。

B.10.5 輸出

有可能並無最符合的情境，但須在結束時對選項範圍，以及指標變化時如何修改其已選擇措施，有比較清楚地認知。

B.10.6 優勢與限制

情境分析考量可能的未來之範圍，其可能

比依賴假設性的高－中－低預測之傳統方式更適合，後者藉由使用歷史資料，認為未來事件可能將持續遵循過去趨勢。此對有關據以預測的目前知識極少，或考慮較長遠的未來之風險等情況係重要的。

然而此優勢具有相關的弱點，即當有高不確定性時，某些情境可能不切實際。

使用情境分析之困難點來自於資料的可取得性，以及分析者與決策者能夠發展出順利產生可能結果之實際情境的能力。

使用情境分析作為決策的工具之危險，為使用之情境可能欠缺充分基礎、資料可能

為純理論的，以及不切實際的結果本身可能不被認同。

B.11 企業衝擊分析(BIA)

B.11.1 一般

企業衝擊分析亦熟知為企業衝擊評鑑，用以分析主要的破壞性風險可能如何影響組織的營運，並鑑別與量化管理所需的能力，特別地，企業衝擊分析提供下列獲得認同的瞭解。

- 重要的產業過程、功能及相關的資源之鑑別與關鍵性，及組織存有主要的相互可恃性。

- 破壞性事件將如何影響達成關鍵企業目標的產能與能力。
- 管理破壞性衝擊並恢復組織到協議的營運水準，所需之產能與能力。

B.11.2 應用

企業衝擊分析用以決定過程相關的資源(人員、設備、資訊技術)之關鍵性與恢復時程，以確保持續達成目標。此外，企業衝擊分析協助決定過程、內部與外部團體，以及供應鏈間的任何聯結之相互可恃性與相互關係。

B.11.3 輸入

輸入包括：

- 執行分析與制定計畫之小組。
- 有關組織的目標、環境、作業及相互可恃性之資訊。
- 有關組織的活動與作業，包括過程、支援資源、與其他組織的關係、外包安排、利害相關者之詳細資料。
- 關鍵性過程失誤所造成之財務與作業後果。
- 備妥之問卷。
- 來自於組織的相關領域及/或將接觸的利害相關者之受訪者名單。

B.11.4 過程

企業衝擊分析可使用問卷、面談、結構化的研討會或所有三者合併進行，以獲得關鍵過程、此等過程失誤之效應，及要求的恢復時程以及支援資源之瞭解。

主要步驟包括。

- 依據風險與弱點評鑑，確認組織的重要過程與輸出，以決定過程之關鍵性。
- 以財務及/或營運的觀點，決定破壞在指定期間內對於所鑑別的關鍵過程產生之後果。
- 鑑別主要的內部與外部利害相關者之相

互可恃性。此可包括透過供應鏈標定出相互可恃性之本質。

- 決定目前可用的資源，與破壞後持續於最低可接受度下營運所需必要的資源水準。
- 鑑別目前使用中或規劃發展的變通辦法與過程，在破壞當中，資源或能力無法取得或不足夠時，可能需發展變通辦法與過程。
- 依據所鑑別出的後果與此功能關鍵的成功因素，決定每一過程之最大可接受違背時間(MAO)。MAO表示組織可忍受能力

損失之最大期間。

目標時間(RTO)。RTO表示組織目標為恢復特殊設備或資訊技術能力範圍內之時間。

- 確認目前管理破壞的關鍵性過程之準備程度。此可包括評估過程中餘裕程度(如備用設備)或存有替代供應商。

B.11.5 輸出

輸出如下列：

- 關鍵過程與相關的相互依存之優先順序清單。
- 來自於關鍵性過程之失誤，已經文件化

的財務與營運影響。

- 經鑑別的關鍵過程所需之支援資源。
- 關鍵過程違背時間架構與相關的資訊技術恢復時間架構。

B.11.6 優勢與限制

企業衝擊分析之優勢包括：

- 瞭解提供組織能力以持續達成其聲明的目標之關鍵過程。
- 瞭解所需的資源。
- 重新界定組織作業過程以協助加強組織恢復力之機會。

限制包括：

- 參與完成問卷、進行面談或研討會的參與者知識不足。
- 團隊活力可能影響關鍵過程之完整分析。
- 恢復的要求期望過於單純或過於樂觀。
- 難以取得組織營運與活動充分的瞭解程度。

B.12 根本原因分析(RCA)

B.12.1 一般

分析主要損失以防止其再度發生的分析，通常稱為根本原因分析(RCA)、根本原因

失效分析(RCFA)或損失分析。根本原因分析專注於因各種類型的失效所導致之資產損失，而損失分析主要關切因外部因素或災禍所導致之財務或經濟損失。根本原因分析不僅僅處理立即可見的癥狀，更試圖鑑別根源或原因。其認知是矯正措施可能並非永遠全盤有效，故有可能需要持續改進。根本原因分析最常應用於主要損失之評估，但亦可用以分析更全面地損失，以決定何處可實施改進。

B.12.2 應用

根本原因分析應用於各種情況，具有下列廣泛的使用領域。

- 以安全為基礎的根本原因分析，用於意外事件調查及職業安全衛生。
- 失效分析使用於技術系統之有關可靠性與維護。
- 以生產為基礎的根本原因分析，應用於工業製造的品質管制之領域。
- 以過程為基礎的根本原因分析，著重於工業過程。
- 以系統為基礎的根本原因分析，經發展用於前述領域的組合，以處理複雜系統

，應用於變動管理、風險管理及系統分析。

B.12.3 輸入

根本原因分析基本的輸入為由失效或損失所蒐集之所有證據，在此分析中亦可考量其他類似失效之資料。其他輸入可能為進行測試特定假設之結果。

B.12.4 過程

當根本原因分析的需求已鑑別後，指派一組專家進行分析並作成建議事項。專家類型大部分依據分析失效所需之特殊專門技術而定。

雖然可使用不同的方法來施行此分析，執行根本原因分析的基本步驟為類似的，且包括：

- 組成小組。
- 建立此根本原因分析之範圍與目標。
- 由失效或損失蒐集資料與證據。
- 施行結構化的分析以決定根本原因。
- 研擬解決方案並做成建議事項。
- 實施此建議事項。
- 確證所實施的建議事項之成功。

結構化的分析技術可包含下列之一。

- 〝5個為何〞技術，即重複詢問〝為何？

〞，以剖析原因與次要原因。

- 失效模式與效應分析(FMEA)。
- 失效(故障)樹分析(FTA)。
- 魚骨圖或要因圖。
- 柏拉圖分析。
- 根本原因圖示。

原因之評估通常由初始顯見的實質原因進展至人為有關之原因，且最終至潛在性管理或基本原因。因果關係之因素必須可由涉及團體予以管制或消除，以使矯正措施有效且值得。

B.12.5 輸出

根本原因分析之輸出包括：

- 蒐集的資料與證據之文件。
- 考量的假說。
- 有關失效或損失最可能的根本原因之結論。
- 矯正措施之建議事項。

B.12.6 優勢與限制

優勢包括：

- 適合的專家參與在團隊環境下工作。
- 結構化之分析。
- 所有可能的假說之考量。
- 結果之文件化。

- 需產生最終建議事項。

根本原因分析之限制包括。

- 所需的專家可能無法取得。
- 關鍵性證據可能在失效中遭到破壞或清理中被移除。
- 小組可能不允許有足夠時間或資源來完全評估情況。
- 可能無法充分地實施建議事項。

B.13 失效模式與效應分析(FMEA)以及失效模式與效應及關鍵性分析(FMECA)

B.13.1 一般

失效模式與效應分析(FMEA)係一種技術，用以鑑別分項、系統或過程可能無法符合其設計目的之途徑。

失效模式與效應分析(FMEA)鑑別：

- 系統各部分所有可能的失效模式(失效模式為觀察到失敗或不正確施行者)。
- 此等失效可能對系統之效應。
- 失效之機制。
- 如何避免此失效，及/或減輕此失效對系統之效應。

失效模式與效應及關鍵性分析(FMECA)擴

展失效模式與效應分析(FMEA)，使逐一所鑑別的錯誤模式依據其重要性或關鍵性排序。

關鍵性分析通常為定性或半定量的，但可使用實際失效發生率予以量化。

B.13.2 應用

有數種FMEA之應用：設計(或產品)FMEA用於零件與產品，系統FMEA用於系統，過程FMEA用於製造與組裝過程，服務FMEA及軟體FMEA。

FMEA/ FMECA可在實體系統的設計、製造或營運中實施。

然而，為改進可恃性，變動通常在設計階段時更易於實施。FMEA與FMECA亦可應用於過程與程序，例如，其用以鑑別保健系統的醫療錯誤之可能性及維護程序中的失效。

FMEA/ FMECA可用以：

- 協助選擇具有高可恃性的設計之替代選擇。
- 確保系統與過程的所有失效模式，及其對作業成功的效應均予以考量。
- 鑑別人為錯誤模式與效應。
- 提供實質系統的規劃測試與維護之基礎

。

- 改進程序與過程之設計。
- 提供如失效(故障)樹分析等分析技術的定性或定量資訊。

FMEA與FMECA可提供如失效(故障)樹分析等其他分析技術定性或定量層面之輸入。

B.13.3 輸入

FMEA與FMECA需要有關系統要項充分詳細的資訊，供有意義的分析每一要項可能失效之方式。對詳細的設計FMEA，要項可為詳細的個別分項層面，而對更高層面的系統FMEA，要項可界定在更高層次。

資訊可包括：

- 進行分析的系統與其分項，或過程的步驟之圖示或流程圖。
- 瞭解過程的每一步驟或系統分項之功能。
- 可能影響作業的環境與其他參數之詳細資料。
- 瞭解特定失效的結果。
- 有關失效，包括可取得的失效率資料之過去資訊。

B.13.4 過程

FMEA過程如下列。

(a)界定此研究之範圍與目標。
(b)召集小組。
(c)瞭解實施FMECA之系統/過程。
(d)此系統細分至其分項或步驟。
(e)界定每一步驟或分項之功能。
(f)對所列的每一步驟或分項，鑑別：
- 每一零件所可預見失效為何？
- 何種機制可能產生此等失效模式？
- 若確實產生失效，效應可能為何？
- 此失效無害或有損害？
- 此失效如何偵測？

(g)鑑別設計中原有的規定以彌補此失效。

對於FEMCA，研究小組繼續對逐項鑑別出的失效模式，依據其關鍵性分類。

有數種方式可以採用，一般的方法包括：

- 模式關鍵性指數。
- 風險等級。
- 風險優先序號。

模式關鍵性係考量中的模式將導致系統整體失效的機率之量測，定義為：

失效效應機率×模式失效率×系統作業時間

其最常應用於設備失效，其中逐項可量化界定，且所有失效模式均具有相同結果。

風險等級係將產生的失效模式結果與失效

機率合併獲得，使用於當不同的失效模式之結果相異時，且可應用於設備系統或過程。風險等級可以定性、半定量或定量表示之。風險優先序數(RPN)為關鍵值的半定量量測，由失效後果評級(通常在1至10之間)、失效可能性評級及偵測此問題的能力之評級等數值相乘計算得之。(若失效不易偵測，則給予較高的優先性)。此方法最常用於品質保證之應用。

一旦失效模式與機制已鑑別，比較顯著的失效模式之矯正措施可予以界定並實施。

FMEA為文件化的報告，包含：

- 分析過的系統之細節。
- 實施演練之方式。
- 分析中所作之假設。
- 資料緣由。
- 結果，包括完成的作業表件。
- 關鍵性(若完成時)與用以界定之方法。
- 進一步分析、設計變更或應納入測試計畫的性能等之任何建議事項。

  在完成行動項目之後，可以另一FMEA循環對係統再予評鑑。

B.13.5 輸出

FMEA之主要輸出為失效模式、失效機制及系統或過程每一分項或步驟的效應之清單(可包括有關失效的可能性之資訊)。亦提出有關失效緣由與對整體系統後果之資訊。FMECA之輸出包括依據系統失效的可能性、導致於失效模式的風險等級，或結合風險等級與失效模式之“可偵測性”分級重要性。

若使用適當的失效率資料與量化後果，FMECA可提供量化之輸出。

B.13.6 優勢與限制

FMEA/FMECA之優勢如下：

- 廣泛應用於人為、設備及系統失效模式，且應用於硬體、軟體及程序。
- 鑑別組成分的失效模式、其緣由與對系統之效應，並以易辨識的方式呈現。
- 透過提早在設計過程鑑別問題，避免使用的設備耗費修改之需要。
- 鑑別單點失效模式並要求複置(redundancy)系統或安全系統。
- 透過強調監測的重要性能，提供發展監測方案之輸入。

限制包括：

- 僅可用以鑑別單一失效模式，而非失效

模式之組合。

- 除非適當地控管與專注於某項目，否則此研究可能耗時與耗費。
- 對複雜的多層面系統可能困難與單調乏味。

B.13.7 參考文件

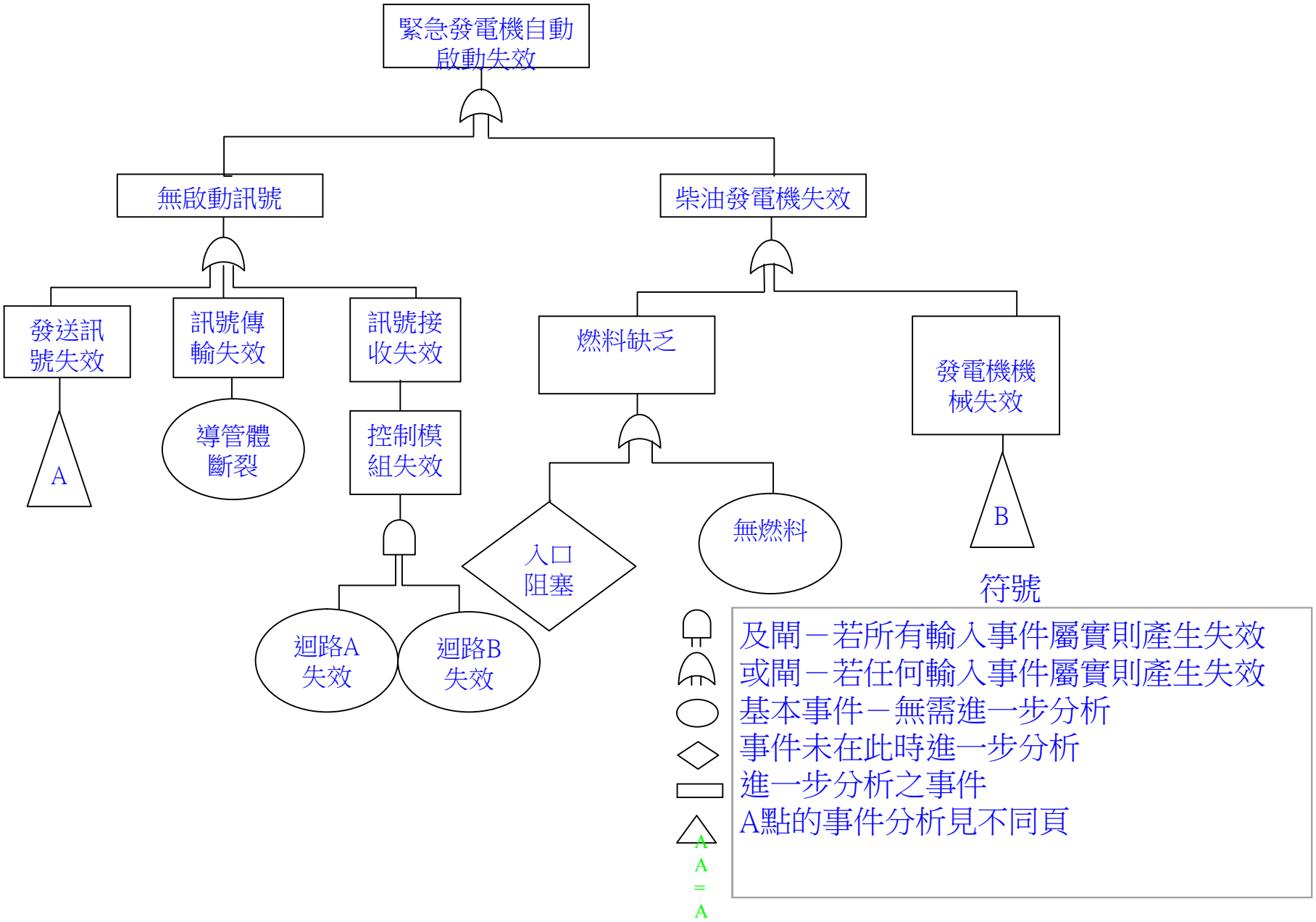
IEC 60812 Analysis techniques for system reliability – Procedures for failure mode and effect analysis (FMEA)

B.14 失效(故障)樹分析(FTA)

B.14.1 一般

失效(故障)樹分析(FTA)係鑑別與分析可造成特定不期望事件(稱為〝頂端事件〞)的因素之一種技術。因果關係的因素經推論鑑別出，以合邏輯的方式組織並圖示於樹狀圖中，以描述因果關係的因素及其與頂端事件之邏輯關係。

失效(故障)樹中所鑑別出的因素可為導致不期望的事件之組成硬體失效、人為錯誤或任何其他相關事件的有關事件。



圖B.2 IEC 60300-3-9之失效(故障)樹分析圖例

B.14.2 應用

可使用失效(故障)樹定性鑑別失效(頂端事件)可能的原因與途徑，或由已知因果關係的事件之機率，定量計算頂端事件之機率。

其可使用於系統的設計階段，以鑑別失效可能的原因，並藉以在不同的設計選項間選擇。其可使用於作業階段，以鑑別主要失效可能如何發生，與主要事件不同的途徑之相對重要性。失效(故障)樹亦可用以分析已發生的失效，圖示不同的事件如何聚集導致失效。

B.14.3 輸入

對於定性分析，需要瞭解系統與失效的原因，以及瞭解此系統在技術上可能如何失效。明細圖有助於協助此分析。

對於定量分析，則需要有關失效比率或所有在失效(故障)樹中的基本事件處於失效狀態之機率資料。

B.14.4 過程

發展失效(故障)樹之步驟如下：

- 界定欲分析的頂端事件，此可為失效或可能為比該失效更廣的後果。在分析後果時，失效(故障)樹可包含減輕有關實

際失效的部分。

- 由頂端事件開始，鑑別導致此頂端事件可能的直接原因或失效模式。
- 逐一分析此等原因/失效模式，以鑑別其失效可能如何造成。
- 繼續跟隨進行至較低的系統層面，逐步鑑別不宜的系統作業，直至無進一步分析之收獲為止。在硬體系統中，此可能為零件失效層面，在所分析的最低系統層面，事件與肇因因素即為基本事件。
- 如機率可分配至基本事件，則頂端事件的機率可計算出。為正確地量化，每一

閘必須足以顯示所有輸入產生輸出事件為必要且充分的。若非此情況，此失效(故障)樹不適用於機率分析，但對於顯示因果關係可係為有用的工具。

在量化之部分，失效(故障)樹可能需予以簡化，使用布林(Boolean)代數來計算重複失效模式。

除提供主要事件機率之估算外，由個別區隔的途徑至主要事件的最小割集可予以鑑別，且其對主要事件的影響可計算出。

除簡單的失效(故障)樹外，當重複事件在

失效(故障)樹的數個位置呈現時，需有套裝軟體來適當的處理計算，並計算最小割集。軟體工具有助於確保一致性、正確性及可確證性。

B.14.5 輸出

失效(故障)樹分析之輸出如下：

- 頂端事件可能如何發生之圖示，顯示必然同時產生的兩個以上事件交互作用之途徑。
- 最小割集之列述(失效之個別途徑)，附帶逐一細分項發生之機率(如資料可取得)。

- 頂端事件之機率。

B.14.6 優勢與限制

失效(故障)樹分析(FTA)之優勢為：

- 其給予高度系統化的訓練方式，但同時允許包括人為互動與實質現象等各種因素分析充分的彈性。
- 應用隱含於技術的〝由上而下〞之作法，集中注意力直接與頂端事件有關的失效效應。
- 失效(故障)樹分析對於分析具有許多介面與交互作用的系統特別有效。
- 圖示引導容易瞭解系統行為與涵蓋的因

素，但由於此失效(故障)樹通常過大，失效(故障)樹處理可能需要電腦系統。此特性使得以涵括更複雜的邏輯關係(如反及邏輯運算(NAND)與反或邏輯運算(NOR))，但亦使失效(故障)樹的確證較為困難。

- 失效(故障)樹中的邏輯分析與割集之鑑別，有助於鑑別極複雜系統中單純失效之途徑，其特殊事件組合引發至頂端事件本有可能受到忽略。

限制包括：

- 基本事件的機率之不確定性涵括於頂端

事件機率之計算中，如基本事件失效機率未能正確認知時，此可導致高層次的不確定度，然而，在充分瞭解的系統中，高可信度係可能的。

- 在某些情況中，肇因事件無法連結一起，且其可能難以確定頂端事件的所有重要途徑是否已涵蓋。例如，以火災作為頂端事件的分析中包括所有起火源，在此情況中，機率分析係不可能的。
- 失效(故障)樹為靜態模式，時間的相互可恃性並未說明。
- 失效(故障)樹僅能處理兩種狀態(失效/

未失效）。

- 當人為錯誤模式可涵括於定性失效(故障)樹時，人為錯誤經常特性的一般程度或品質失效並無法輕易囊括。
- 失效(故障)樹無法輕易涵盖骨牌效應或條件式失效。

B.14.7 參考文件

IEC 61025 Fault tree analysis (FTA)
IEC 60300-3-9 Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systemes

B.15 事件樹分析(ETA)

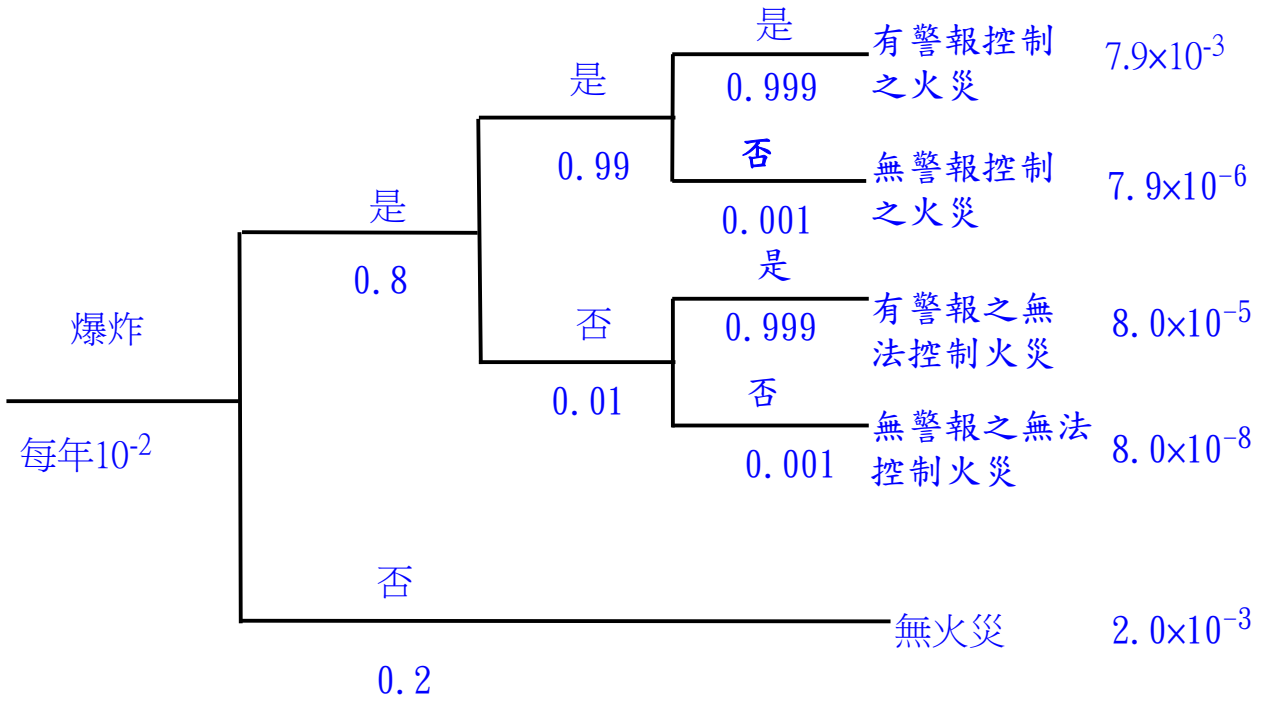
B.15.1 一般

事件樹分析(ETA)是一種圖解技術，可用以顯示某一起始事件之後續事件相互之間排他性，依所設計用以緩解其影響的各種系統之運作功能/不運作功能(參照圖B.3)。此一方法不論定性與定量皆可應用。

圖B.3顯示當樣本事件樹之各分枝為完全獨立時之簡單的計算案例。

藉由樹狀的展開，事件樹分析得以在考量附加的系統、功能或障礙之下，表示回應起始事件之惡化或減輕的事件。

起始事件	著火	灑水系統作用	火災警報器啟動	後果	頻率（每年）



圖B.3　事件樹圖例

B.15.2　應用

事件樹分析可用以模式化、計算及分級(由風險觀點)起始事件隨後不同的意外事件情境。

事件樹分析可用於產品或過程的生命週期之任何階段。其可定性使用以協助對起始事件隨後的事件之可能情境與順序作腦力激盪，以及後果如何受到意圖減輕不期望後果之各種處理、障礙或控管之影響。

定量分析對於控管可接受性之考量有用處。最常用以模式化具有多重安全保障的失效。

事件樹分析可用以模式化可能帶來損失或增益的起始事件，然而，尋求最適的增益途徑之狀況，較常使用決策樹予以模式化。

B.15.3 輸入

輸入包括：

- 適當的起始事件之清單。
- 有關處理、障礙及控管以及其失效機率(供定量分析)之資訊。
- 對起始失效事件擴散過程之瞭解。

B.15.4 過程

事件樹由選擇起始事件著手，此可能為例如粉塵爆炸之事故或如電力失效之肇因事件。然後依序列出用以減輕後果所具備的功能或系統，對每一功能或系統，拉出代表其成功或失效之直線，失效之特定機率可分配至每一直線，依據此估算的條件機率，如透過專家判斷或失效(故障)樹分析，依此方式，源於起始事件的不同途徑得以模式化。

注意有關事件樹的機率為條件機率，例如，引起灑水系統動作之機率並非正常狀況下試驗所獲得機率，而是由於爆炸造成的

火災狀況下起作用之機率。

經此失效(故障)樹之每一途徑代表在此途徑中所有事件將發生的機率。因此，設定各事件各簡獨立其後果之頻率以個別狀況的機率與起始事件頻率之乘積表示之。

B.15.5 輸出

事件樹分析之輸出包括下列：

- 將始自起始事件產生各種類型的問題(後果之範圍)之事件組合作為潛在的問題之定性描述。
- 事件頻率或機率之定量估算，以及各種失效序列與促成事件之相對重要性。

- 降低風險建議事項清單。
- 建議事項有效性之定量評估。

B.15.6 優勢與限制

事件樹分析之優勢包括下列：

- 事件樹分析以清楚的圖示方式顯示起始事件隨後之可能情境，及緩解系統或功能成功或失效之影響。
- 可考量難以模式化處理於失效(故障)樹內之時間安排、可恃性及骨牌效應。
- 以圖解表示使用失效(故障)樹不可能表現的事件序列。

限制包括：

- 為使用事件樹分析作為全面性評鑑之一部分，所有可能的起始事件需予以鑑別，此可使用另一種分析方法[如危害與可操作性研究(HAZOP)、初期危害分析(PHA)]進行，然而，經常有失誤某些重要起始事件之可能性。
- 事件樹分析僅處理系統的成功與失效狀態，且其難以納入延遲的成功或恢復之事件。
- 任何途徑限制於先前沿此途徑的分枝點曾發生的事件，許多沿此途徑之可恃性因而提出。然而，某些如共同元件、公

用系統及操作者等可恃性，若未小心處理可能忽略掉，可能導致過於樂觀估計風險。

B.16 因果分析

B.16.1 一般

因果分析係失效(故障)樹與事件樹分析之組合，因果分析由關鍵性事件開始並藉由〝是/否〞邏輯閘組合之方式分析結果，〝是/否〞閘係為緩解起始事件後果的系統可能有作用或失效狀況之表示。狀況有作用或失效之緣由透過失效(故障)樹工具

予以分析(參照B.15)。

B.16.2 應用

因果分析最初發展作為安全關鍵性系統之可靠性工具，以提供系統失效更完整的瞭解。類似失效(故障)樹分析，因果分析用以表示導致關鍵事件的失效邏輯，但加入失效(故障)樹之功能性，使得以分析依時間順序之失效。此方法亦使時間延遲得以納入後果分析中，而事件樹分析並不能用此法。

此方法用以分析關鍵事件隨後系統可能採取之各種途徑，並依據特定次系統(如

緊急應變系統)的行為而定。若量化後將提供關鍵事件隨後不同的可能後果機率之估算。

由於因果圖之每一序列係次失效(故障)樹的組合，故此因果分析可作為建立大型失效(故障)樹之工具。

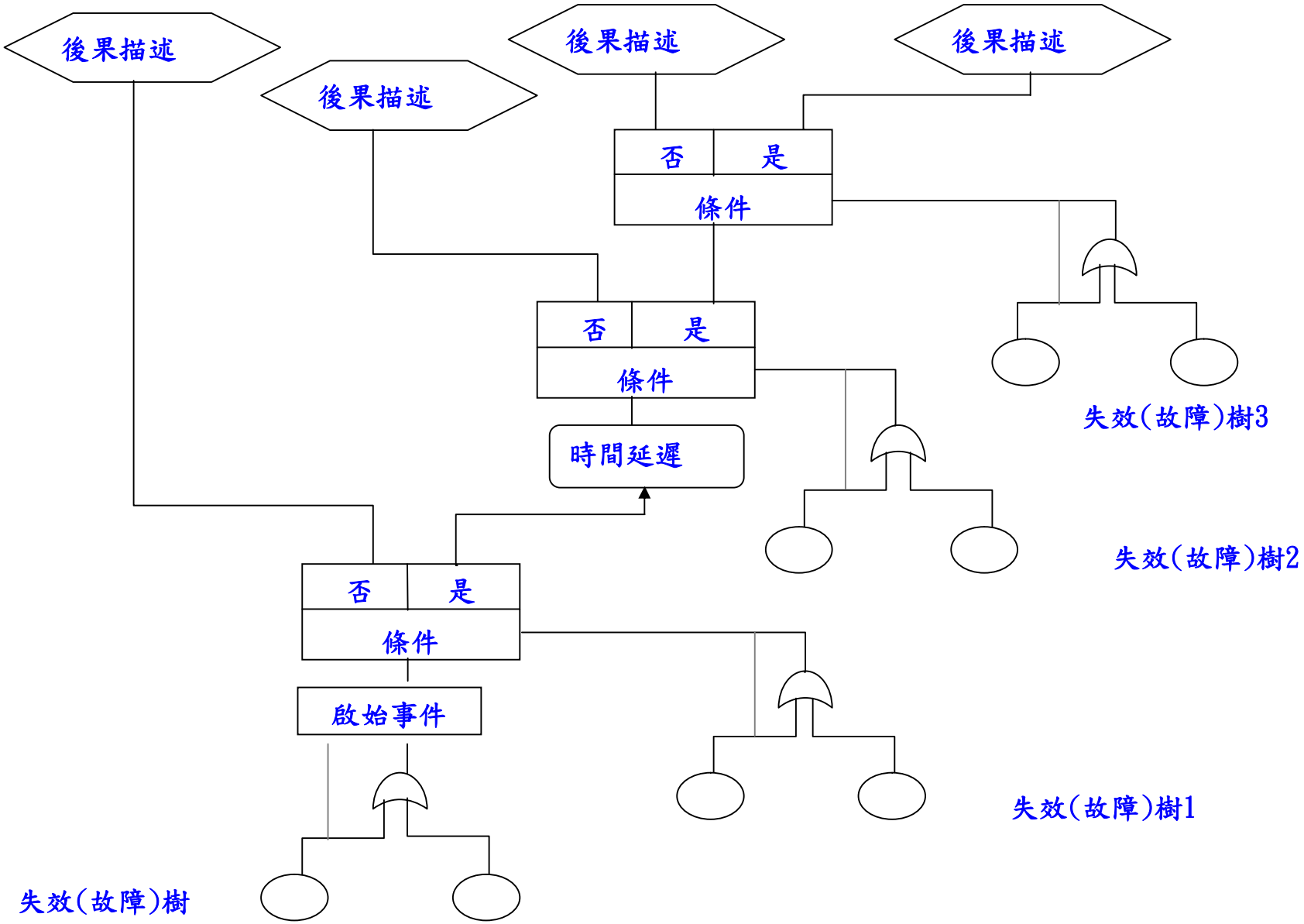
圖製作與使用複雜，且傾向於當失效可能的後果之大小，證實為密集的努力時使用。

B.16.3 輸入

對系統與其失效模式及失效情境的瞭解有其必要性。

B.16.4 過程

圖B.4顯示典型的因果分析之概念圖。


後果描述
後果描述
後果描述
後果描述
否
是
條件
否
是
條件
時間延遲
否
是
條件
啟始事件
失效(故障)樹
失效(故障)樹1
失效(故障)樹2
失效(故障)樹3

圖B.4　因果分析圖例

程序如下列：

(a)鑑別關鍵性(或起始)事件(相當於失效(故障)樹的頂端事件與事件樹之起始事件)。

(b)依B.14所述發展與確證失效(故障)樹起始事件之原因，使用如傳統的失效(故障)樹分析之相同符號。

(c)決定考量的狀況之順序，此須為依其發生的時間順序有條理的序列。

(d)依據不同的狀況建構後果之途徑。此類似事件樹，但此事件樹的途徑之分叉顯示如一方框，標示適用的特殊狀況。

(e)倘若每一狀況方框之失效為獨立的，每一後果之機率可予以計算出，由初次分配至狀況方框每一輸出之機率得到(適當時使用相當的失效(故障)樹)，導致特定後果的任一序列之機率由狀況在該特定後果終止的逐一序列機率之乘積而得。若超過一序列在終止時具有相同後果，則每一序列之機率應相加。若在序列的狀況失效之間有可恃性(例如電力失效可能造成數種失效狀況)，則此可恃性在計算之前須予以處理。

B.16.5 輸出

因果分析之輸出為顯示系統可能如何失效的原因與後果之圖示。每一可能的後果依據關鍵性事件之後，分析特定狀況發生機率，估算其發生之機率。

B.16.6 優勢與限制

因果分析之優點與事件樹及失效(故障)樹合併者相同，此外，因果分析克服些等技術之一些限制，得以分析歷經時間發展之事件，因果分析提供系統全面性的觀點。

因果分析的限制在於相較於失效(故障)樹與事件樹分析更為複雜，兩者的建構與方

均為於量化過程中之處理其可恃性。

B.17 原因與效應分析

B.17.1 一般

原因與效應分析係鑑別不期望事件或問題可能的原因之結構化方法。其將可能的促成因素有系統的區分為廣泛類別，使得以考量所有可能的假設。然而，其本身並不指出實際的原因，因此等僅能由實際證據與假設之實驗性測試決定。此資訊以魚骨圖(亦稱要因圖)或有時以樹狀圖(參照B.17.4)予以系統化。

B.17.2 應用

原因與效應分析提供特定效應的原因之結構化圖示，效應依其情況可為正面(目標)或負面(問題)。

其的使用得以考量由專家小組產生的所有可能情境與原因，並使對最可能的原因之共識得以建立，然後可實驗測試或由可取得資料評估。其在分析開始時擴展有關可能原因之思維最有效，並且在其後建立可更正式考量的可能性假設。

當有下列需求時可進行建構原因與效應圖。

- 鑑別特定效應、問題或狀況可能的根本原因、基本理由。
- 歸納與串聯某些影響特定過程的因素間之相互作用。
- 分析目前的問題使得以採取矯正措施。

建構原因與效應圖之益處包括：

- 聚集審查成員對特定問題之注意力。
- 使用結構化方式協助決定問題之根本原因。
- 激勵團隊參與並利用團隊有關產品或過程之知識。
- 使用有次序、易於判讀的格式繪製原因

與效應關係。

- 指出過程中的變異之可能原因。
- 鑑別進一步研究須蒐集的資料之領域。

原因與效應分析可用作為施行根本原因分析(參照B.12)的方法。

B.17.3 輸入

原因與效應分析之輸入可來自於參與者的專業知識與經驗，或曾在過去使用之先前發展之模式。

B.17.4 過程

原因與效應分析須由一組熟知需解決的問題之專家進行。

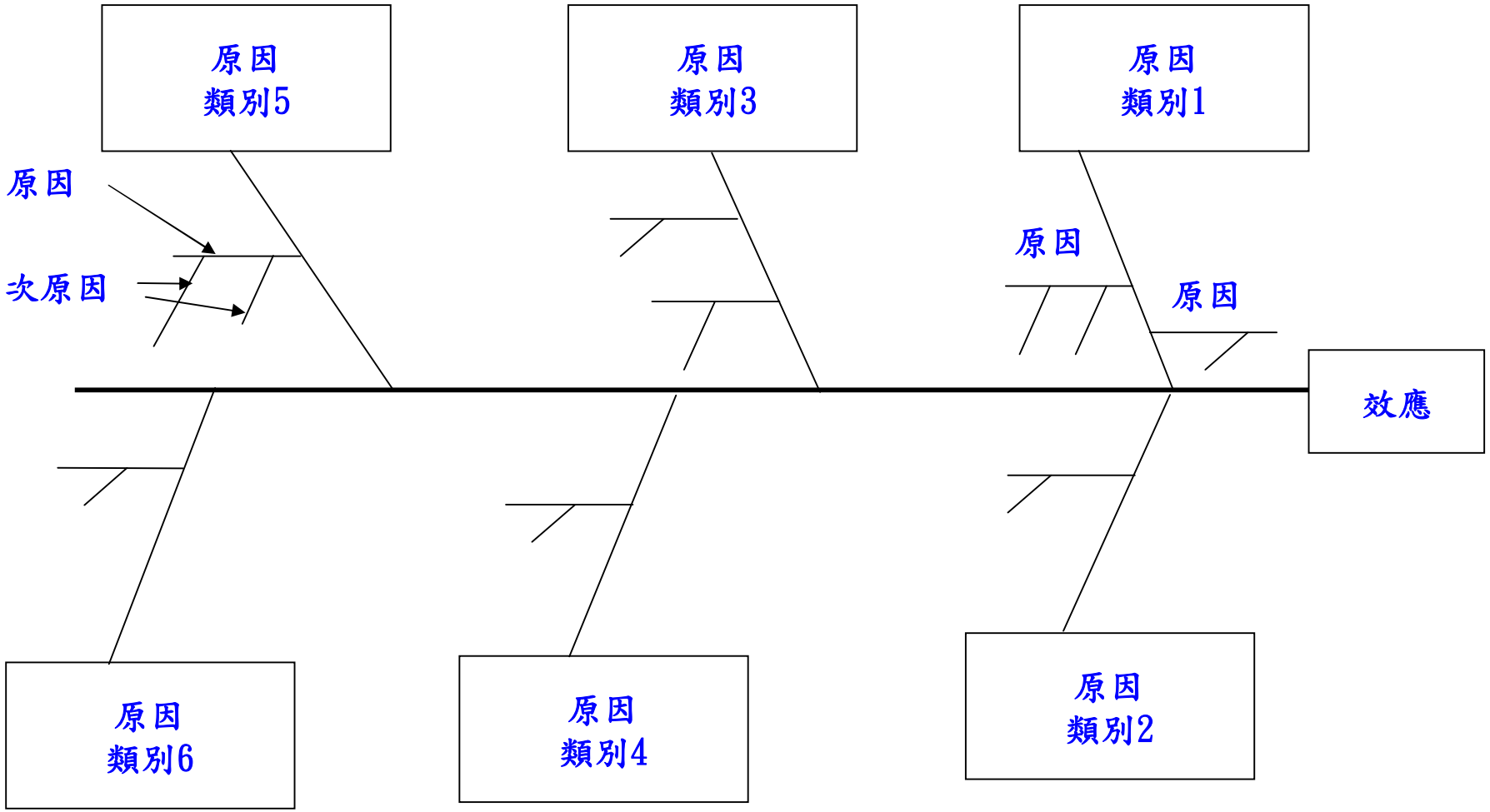
施行原因與效應分析之基本步驟如下列：

- 建立欲分析之效應並寫入框內，效應依其情況可為正面(目標)或負面(問題)。
- 決定原因之主要分類，以方框表示於魚骨圖中。基本上，對於系統問題，分類可為人員、設備、環境、過程等，然而，此需配合特定情況選定。
- 填寫每一主要分類可能的原因，以分枝與次分枝來描述相互間之關係。
- 持續詢問〝為何？〞或〝原因何在？〞來連結原因。
- 審查所有分枝以確證一致性與完整性，

並確使原因適用於主要效應。

- 依據小組之意見與可取得證據，鑑別最可能的原因。

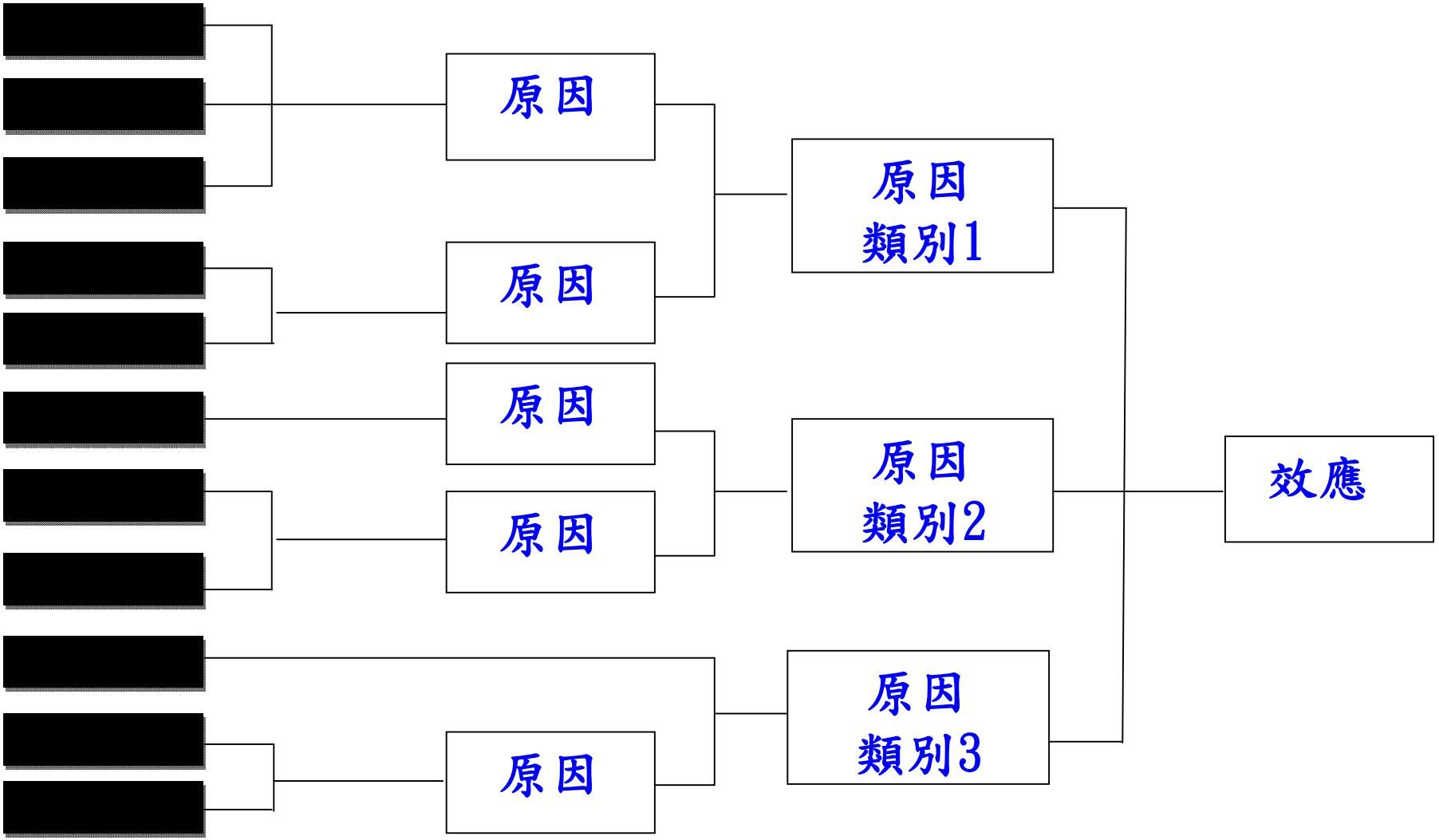
後果通常以魚骨圖或要因圖或樹狀圖展開。魚骨圖係以個別原因納入主要分類構造之(以魚的背脊骨分枝之直線表示)，分枝與次分枝描述此等分類更特定之原因。



圖B.5　要因圖或魚骨圖圖例

樹狀表示法外觀類似失效(故障)樹，惟通常其係由左至右樹狀展開，而非由上至下。然而，其無法量化產生主要事件之機率，因其原因為可能的促成因素，而非已知發生機率的失效。

原因與效應圖通常為定性使用，其可能假設問題之機率為1，並將機率分配至概括原因，繼而以有關其相關性的信心度為基礎，分配至次要原因。然而，促成因素通常可相互作用並以複雜的方式促成效應，使量化無效。



圖B.6 原因與效應分析之樹狀系統陳述圖例

B.17.5 輸出

原因與效應分析之輸出為顯示或許是與可能的原因之魚骨圖或樹狀圖，在後來作成建議事項之前，須予以確證並實驗測試。

B.17.6 優勢與限制

優勢包括：

- 適合的專家參與在小組環境中工作。
- 結構化的分析。
- 考量所有可能的假設。
- 圖示易於瞭解的後果。
- 鑑別出需要進一步資料輔助的領域。
- 可用以鑑別期望以及非期望的效應之促

成因素，採取明確聚焦在可鼓勵更大的自主與參與之議題。

限制包括：

- 小組可能不具備必要的專業知識。
- 其本身並非完整過程而需作為根本原因分析之一部分，以產生建議事項。
- 與其說其是個別分析技術，不如說其是腦力激盪之展現技術。
- 在分析開始時區分因果關係之因素為主要類別，意味類別相互間之作用可能未能適切考量，如設備失效係由人為錯誤導致，或人為問題之導因為不良之設計。

B.18 保護層分析(LOPA)

B.18.1 一般 。

保護層分析(LOPA)係估計與不期望的事件或情境有關的風險之半定量方法。其分析是否有充分的技施控管或減輕風險。

選擇因果配對並鑑別出防止導致不期望後果的原因之保護層，進行數值之冪次的計算以決定此保護是否足以降低風險至可忍受程度 。

B.18.2 應用

保護層分析可單純的定性使用來審查危險

或肇因事件與後果之間的保護層。通常應用半定量方式以增進例如危害與可操作性研究(HAZOP)、初期危害分析(PHA)之後更嚴格的篩選過程。

依IEC 61508系列與IEC 61511標準所述，保護層分析提供所配置的系統獨立保護層(IPLs)與安全完整度(SIL)的規範之基礎，決定所配置安全系統的安全完整度(SIL)要求。保護層分析可藉由分析每一保護層產生的風險減降，用以協助分配有效的風險減降之資源。

B.18.3 輸入

保護層分析之輸入包括：

- 有關風險之基本資訊，包括如透過初期危害分析(PHA)所提出的危險、緣由及後果。
- 有關已具備或提議的控管之資訊。
- 肇因事件之頻率，與保護層失效機率、後果採行措施及容許風險之界定。
- 產生原因之頻率、保護層失效機率後果採行措施及容許風險之界定。

B.18.4 過程

保護層分析使用一專家小組應用下列程序進行。

- 鑑別不期望的後果之產生原因，並尋找有關其頻率與後果之資料。
- 選擇單一因果配對。
- 鑑別出防止造成不期望結果的行為之保護層，並分析其有效性。
- 鑑別獨立保護層(IPLs)(並非所有保護層皆為IPLs)。
- 估計每一獨立保護層之失效機率。
- 產生原因之頻率，與每一獨立保護層之失效機率及任何有條件的修正因子(調整

的修正因子例如現場是否有人員受到影響)之機率合併，以決定不期望後果產生之機率。頻率與機率以其數值之冪次計量。

- 計算出的風險等級與風險容忍度比較，以決定是否需要進一步的保護。

  獨立保護層(IPL)為足以防止情境邁入不期望後果之裝置的系統或行動，與肇因事件或與此情境相關的任何其他保護層無關。

獨立保護層(IPL)包括：

- 設計之特徵。

- 實體保護裝置。
- 連鎖裝置與停機系統。
- 重要的警報與手動介入裝置。
- 事件後之實質保護。
- 緊急應變系統(程序與檢查並非獨立保護層)。

B.18.5 輸出

應提出任何進一步控管與此等控管降低風險的有效性之建議事項。

保護層分析(LOPA)係當涉及安全有關/裝置的系統之安全裝置等級(SIL)評鑑使用的技術之一。

B.18.6 優勢與限制

優勢包括：

- 其所需的時間與資源較失效(故障)樹分析或全定量風險評鑑少，但較定性的主觀判斷更為正確。
- 其協助鑑別與集中資源於最關鍵的保護層。
- 其鑑別具有不足夠的安全保護之營運、系統及過程。
- 其著重於最嚴重的後果。

限制包括：

- 保護層分析(LOPA)著重於一次一個因果

配對與一項情境，未能涵括風險或控管間複雜的相互作用。

- 量化的風險可能未考慮到一般模式之失效。
- 保護層分析(LOPA)不適用於具有許多因果配對，或具有影響不同的利害相關者多種後果之極複雜情境。

B.18.7 參考文件

IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511 Fuctional safety – Safety instrumented systems for the process industry sector

B.19 決策樹分析

B.19.1 一般

決策樹係為在考量不確定結果之下，以依序之方式表示決策之替代方案與後果。決策樹分析類似於事件樹由產生事件著手，或依初始的決策與模式之不同途徑與後果，作為事件可能發生之後果，且可作成不同的決策。

B.19.2 應用

決策樹用以管理專案的風險，且在其他狀況下，協助選擇具有不確定性的行動之最佳途徑。圖示方式顯現亦可協助溝通決策之理由。

B.19.3 輸入

附帶決策點之專案，有關決策之可能結果及有關可能影響決策的機遇性事件等資訊。

B.19.4 過程

決策樹由初始決策著手，例如與其進行專案B不如進行專案A。當兩個假設性專案進行

時，將產生不同的事件，且將需達成可預測的不同決策。此類似事件樹，表示於樹狀格式中，事件之機率可連同此途徑最終的結果的成本或可用性予以估算出。

有關最佳決策途徑之資訊系有條理的，其產生頂端預期值，以依此途徑的所有狀況之機率與後果值之乘積計算出。

B.19.5 輸出

輸出包括：

- 有條理地分析風險，展現可採取之不同選項。
- 逐一計算可能的途徑預期值。

B.19.6 優勢與限制

優勢包括：

- 提供決策問題細節的清楚代表圖示。
- 得以計算經由一情況的最佳途徑。

限制包括：

- 大型決策樹可能過於複雜，不易與其他人員溝通。
- 為使得以在樹狀圖表示，可能傾向於過於簡化面對此情況。

B.20 人因可靠度評鑑(HRA)

B.20.1 一般

人因可靠度評鑑(HRA)論及人類對系統績效的影響，並可用以評估人為錯誤對系統之影響。

許多過程含有人為錯誤之可能性，尤其是當操作者作成決策可用的時間短絀時。問題將足夠發展至形成嚴重性之機率可能極小，然而，有時人類的行動將為防止初始失效進展至意外事件僅有的防線。

人因可靠度評鑑(HRA)的重要性透過各種意外事件予以說明，在其中關鍵性人為錯誤造成事件的災難性不幸結果。此等意外為對僅著重於系統中的硬體與軟體之風險

評鑑提出警告，其們說明忽視人為錯誤造成的可能性之危險。更且，人因可靠度評鑑有助於突顯可能阻礙生產力之錯誤，並以啟發性的方式強調此等錯誤與其他失效(硬體與軟體)，可由人類的操作者與維護人員予以“回復”。

B.20.2 應用

人因可靠度評鑑(HRA)可定性或定量使用，定性時，用以鑑別人為錯誤之可能性與其原因，使錯誤之機率得以降低。定量時，人因可靠度評鑑可用以對失效(故障)樹分析(FTA)或其他技術提供人為失效之資

料。

B.20.3 輸入

人因可靠度評鑑(HRA)之輸入包括：

- 界定人員須執行的工作之資訊。
- 實務上發生的錯誤類型與錯誤的可能性之經驗。

有關人為錯誤與其量化之專業知識。

B.20.4 過程

人因可靠度評鑑(HRA)之過程如下。

- 問題界定，何種類型的人為牽連事項需要調查/評鑑？

- 工作分析，工作將如何執行以及需有何種型式的協助以支持工作執行？
- 人為錯誤分析，任務成效可能如何失效：何種錯誤可能發生以及何予以回復？
- 代表性，此等錯誤或任務成效失效可如何與其他硬體、軟體及環境事件整合，以計算出整體系統失效之機率？
- 篩選，是否有任何錯誤或工作並不需要詳細的量化？
- 量化，個別錯誤與工作之失效可能性如何？
- 影響評鑑，何項錯誤或工作最重要，即

何者對可靠度與風險具有頂端的貢獻度？

- 錯誤降低，如何達成更高的人因可靠度？
- 文件化，人因可靠度評鑑(HRA)之細節何者需予以文件化？

  實務上，人因可靠度評鑑(HRA)之過程，雖然有時部分(如工作分析與錯誤鑑別)與其他部分同時進行，但其係逐步地進行。

B.20.5 輸出

B.20.5 輸出

輸出包括：

- 可能產生的錯誤及其可予以降低之方法一覽表－最好透過系統的重新設計。
- 錯誤模式、錯誤類型之原因與後果。
- 錯誤所引起的風險之定性或定量評鑑。

B.20.6 優勢與限制

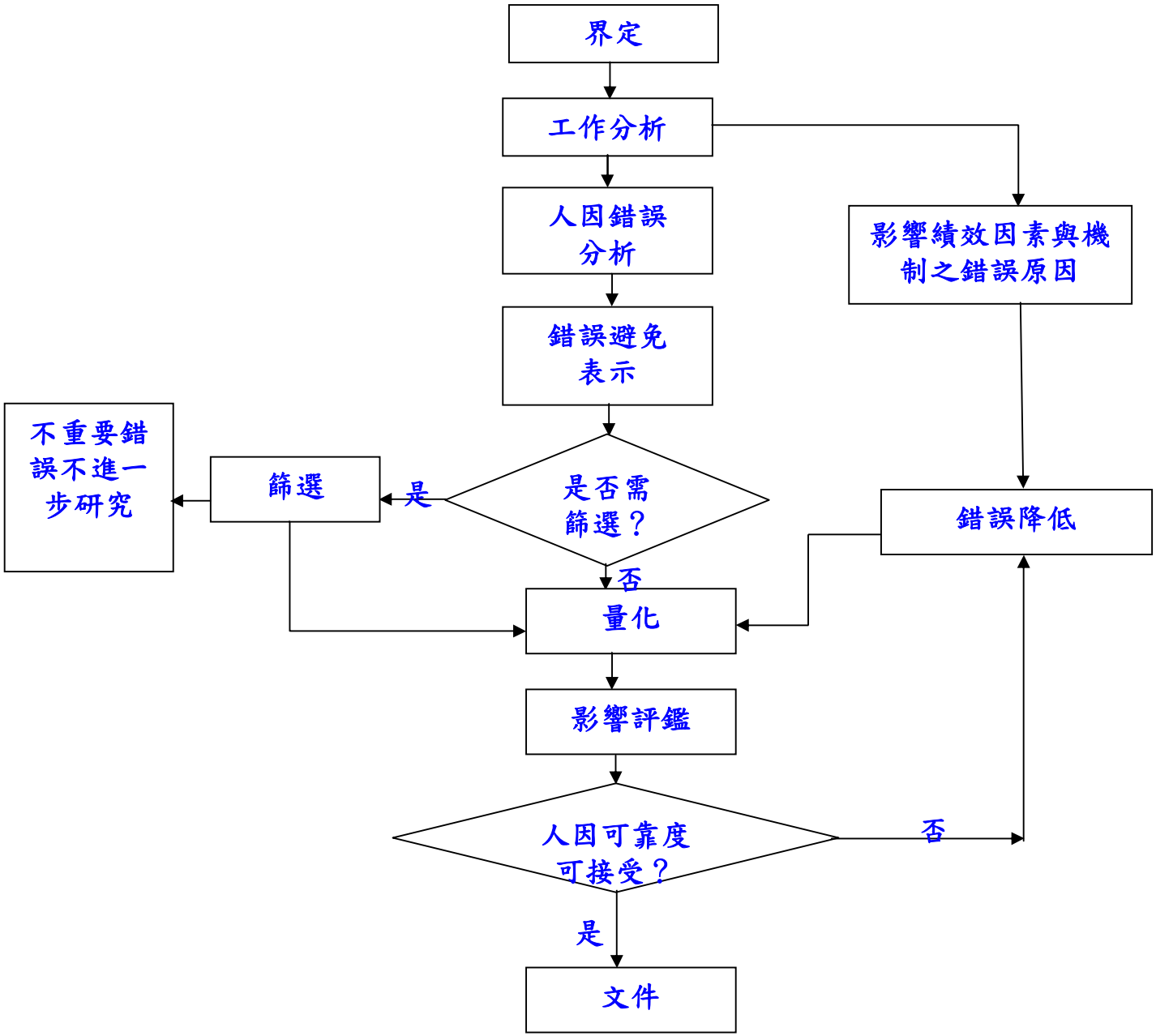
人因可靠度評鑑(HRA)之優勢包括：

- 人因可靠度評鑑(HRA)提供正式的機制，包括考量與系統有關的風險時，人類經常扮演重要角色的人因錯誤。
- 正式的考量人因錯誤模式與機制，可協

助降低因錯誤而失效的機率。

限制包括：

- 人類的複雜性與變異性，使難以界定簡單的失效模式與機。
- 許多人類的活動並不具有簡單的符合/不符合模式，人因可靠度評鑑(HRA)在處理部分失效或品質失效或不良決策訂定，具有其困難度。



圖B.7　人因可靠度評鑑圖例

B.21 蝴蝶結分析

B.21.1 一般

蝴蝶結分析為描述與分析風險由原因至後果的途徑之簡單圖示方式。其可考量為失效(故障)樹分析事件(以蝴蝶結之結點表示)的原因與事件樹分析後果的思維之合併。然而，蝴蝶結的重點在於原因與風險，以及風險與後果之間的障礙。蝴蝶結圖建構可由失效與事件樹著手，但更通常係直接由腦力激盪部分得出。

B.21.2 應用

蝴蝶結分析係用以展現顯示可能的原因與後果範圍之風險。其在無法保證完全以失效(故障)樹分析複雜性之情況使用，或當更著重於確使每一失效途徑具有障礙或控管時使用。當對具有清楚導致失效的獨立途徑，係有幫助的。

蝴蝶結分析通常較失效與事件樹更易於瞭解，且因此當使用更複雜的技術達成分析時，可為一項有效的溝通工具。

B.21.3 輸入

瞭解有關風險的原因與後果，以及可防止、減輕或刺激風險的障礙與控管之資訊，

係需要的。

B.21.4 過程

蝴蝶結依下述繪製。

(a)鑑別出一特定風險進行分析，並表示為蝴蝶結的中心結點。

(b)考量風險(或安全情況中的危險)之緣由，列出事件之原因。

(c)鑑別風險緣由導致關鍵事件之機制。

(d)每一緣由與事件之間連線形成蝴蝶結之左側，可能導致提升的因素可予以鑑別並包括在圖內。

(e)防止每一緣由導致不期望後果之障礙，

可在線上以垂直棒狀物顯示。如有可能導致提升的因素，對提升之障礙亦可表示出。此方式可用於正面後果，此時該棒狀物反映刺激事件產生的〝控管〞。

(f)在蝴蝶結之右側，鑑別出風險不同的可能後果，並由逐一可能的後果之風險事件繪輻射狀連線。

(g)後果之障礙在輻射狀連線上以棒狀物描述，此方式可用於正面後果，此時該棒狀物反映支援後果產生的〝控管〞。

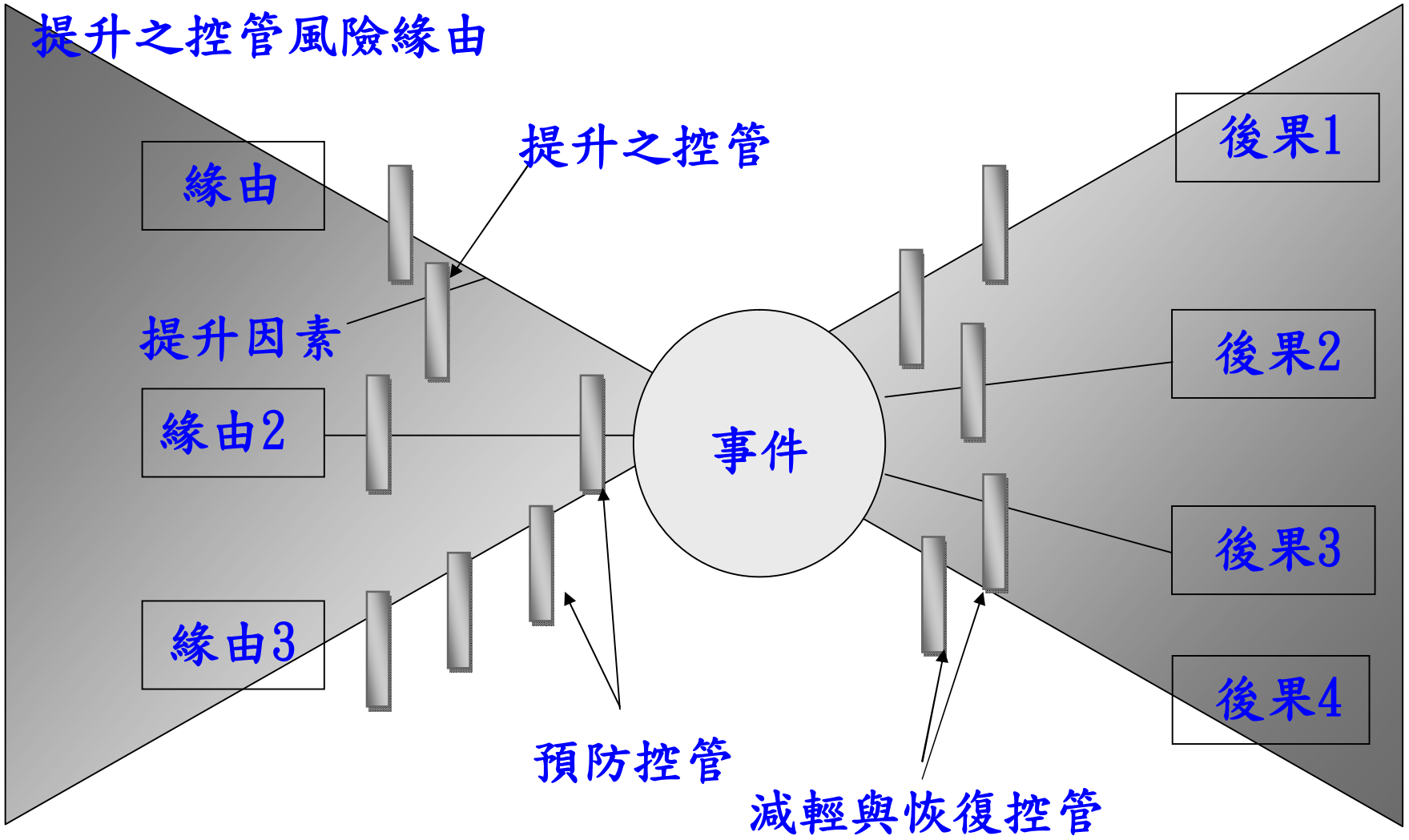
(h)支援控管的管理功能(如訓練與檢查)可在蝴蝶結下方顯示出，並連接至相對應

的控管。

如途徑為獨立時，蝴蝶結圖某種程度的量化係可行的，已知特定後果或後果之機率，且控管有效性之數值可予以估算出。然而在許多情況下，途徑與障礙並非獨立的，且控管可能為依序的，因此其有效性不明確。量化通常使用失效(故障)樹分析(FTA)與事件樹分析(ETA)進行較為適當。

B.21.5 輸出

輸出為一簡單的圖形，顯示防止或減輕不期望的後果，或刺激與促進期望的後果所具備的主要風險途徑與障礙



圖B.8　不期望的後果蝴蝶結圖圖例

B.21.6 優勢與限制

蝴蝶結分析之優勢為：

- 易於瞭解並提出問題清楚的圖示。
- 集中注意力於預期已具備可同時預防與減輕之控管，及其有效性之控管。
- 可用以得到期望的後果。
- 不需使用高水準的專業知識。

限制包括：

- 無法描述導致後果同時發生的多重原因（ 即描述於蝴蝶結左側的失效(故障)樹中具有及閘)。

- 可能過於單純化複雜之情況，尤其是在嘗試量化時。

B.22 可靠度中心維護(RCM)

B.22.1 一般

以可靠度為中心之維護係鑑別須實施以管理失效的政策之方法，以使有效能與有效率地達成所要求之所有類型的設備操作之安全性、可用性及經濟性。

以可靠度為中心之維護現已為經確證與接受的方法，廣泛使用於產業範圍。

以可靠度為中心之維護提供決策過程，該過程依據可鑑別的失效之安全、作業及

及經濟後果，以及歸責於此類失效的退化機制，鑑別設備可適用的與有效的預防維護要求。此過程的作業之最終結果，為對實施維護工作或如採行其他措施如作業變動所作之判定。有關可靠度中心維護(RCM)的使用與應用之詳細資料提供於IEC 60300-3-11中。

B.22.2 應用

所有工作係以針對人員與環境之安全，及作業上或經濟上關心的事項為基礎。然而，須注意的是所考量的準則將依據產品與其應用之本質而定，例如，製造過程需為

經濟上可實施的，並可能對嚴格的環境考量面敏感，然而防衛型設備項目須成功地作業，但卻可能具備較不嚴格的安全、經濟及環境準則。透過瞄準失效將嚴重影響安全、環境、經濟或作業效果進行分析，可達成最大的獲益。

可靠度中心維護(RCM)用以確保已施行適合與有效的維護，且通常應用於設計與發展階段時，並在其後於營運與維護時實施。

B.22.3 輸入

成功的可靠度中心維護(RCM)之應用，需要深入瞭解設備與結構、作業環境與相關的

系統、次系統及裝備的機件項目，併同可能的失效以及此等失效之後果。

B.22.4 過程

可靠度中心維護(RCM)方案依下列之基本步驟。

- 發起與規劃。
- 功能失效分析。
- 任務選定。
- 實施。
- 持續改進。

由於可靠度中心維護(RCM)遵循風險鑑別之基本步驟，故其係以風險為基礎。風險

評鑑之型式為失效模式、效應及關鍵性分析(FMECA)，但使用於此情況時需有特定的分析方式。

風險鑑別著重於潛在的失效頻率及/或後果，藉由進行維護工作可予以消除或降低的情況。透過鑑別所要求的功能與性能標準，及可能阻擋此等功能的設備與零件之失效執行之。

風險分析包含無實施維護的逐一失效頻率之估算，透過界定失效效應建立後果，結合失效頻率與後果的風險矩陣，得以建立風險等級之種類。

然後選擇每一失效模式適當的失效管理政策施行風險評估。

完整的可靠度中心維護(RCM)過程詳盡地文件化，以供未來參考與審查。失效與維護有關的資料之蒐集得以監測後果與實施改進措施。

B.22.5 輸出

可靠度中心維護(RCM)提供如狀況監測、預定的恢復、預定的替換、失效調查或非預防性維護等維護工作之界定。其他由此分析可產生的可能措施，包括重新設計、操作或維護程序之變動或附加的訓練，其後

鑑別工作時程以及所需的資源。

B.22.6 參考文件

IEC 60300-3-11 Dependability management – Part 3-11: Application guide – Reliability centred maintance

B.23 潛行分析(SA)與潛行路徑分析(SCA)

B.23.1 一般

潛行分析(SA)為鑑別設計錯誤的方法。潛行狀況係指可能導致產生不希望的事件或

可能抑止不期望的事件，且並非因零件失效所導致的潛伏硬體、軟體或整體之狀況。這些狀況之特徵為其隨機之特性，且當以最嚴厲的標準化系統測試時，有能力避開偵測。潛行狀況可導致不當的操作、系統可用度之損失、預定工作遲延，或甚而造成人員的死亡或傷害。

B.23.2 應用

潛行路徑分析(SCA)由美國航空太空總署(NASA)於1960年代末期發展，用以確證其設計之完整性與功能性。其作為發現非故意的路徑途徑係有效的工具，並協助區分

解決方案以區隔每一項功能。然而，因科技增進，潛行路徑分析之工具亦須提升，潛行分析(SA)包括且遠超過潛行路徑分析(SCA)之涵蓋範圍，其可使用任何技術同時找出硬體與軟體之問題。潛行分析(SA)工具可整合如失效(故障)樹、失效模式與效應分析(FMEA)、可靠度估計等數種分析法為單一分析以節省時間與專案費用。

B.23.3 輸入

潛行分析(SA)獨特於設計過程的是，其使用不同的工具(網狀樹甚或樹林，與線索或問題來協助分析者鑑別潛行狀況)找出

特定型式的問題。網狀樹甚或樹林為實際系統的形態歸類，每一網狀樹代表一次功能，並顯示可能影響次功能輸出的所有輸入。樹林係結合有助於特定系統之網狀樹建構而成，適當的樹林以其所有有關的輸入來顯示系統之輸出，此等輸出與其他輸出結合，成為此分析的輸入。

B.23.4 過程

施行潛行分析之基本步驟包括：

- 資料準備。
- 網狀樹之建構。
- 網狀途徑之評估。

• 最終建議事項與報告。

B.23.5 輸出

潛行路徑為系統內意想不到的途徑或邏輯流，其在某些情況下，可能發動不期望的功能或抑制期望的功能。此途徑可能包含硬體、軟體、操作者措施或此等要素之組合。潛行路徑並非硬體失效後果，而是潛伏狀況疏忽地設計於系統中，編碼於軟體程式中，或由人為錯誤所引起。有四種類型的潛行路徑。

(a)潛行途徑：

能量或邏輯序列沿著意想不到的途徑流

入非預期的方向。

(b)潛行時機：

事件依非預期或矛盾的序列發生。

(c)潛行癥狀：

系統操作狀況模糊不清或錯誤的顯示，可能造成系統或操作者採取不預期之措施。

(d)潛行標示：

不正確或不精確的系統功能標示，如系統輸入、控制器、顯示訊息通道，其可能導致操作者對系統施加不正確的刺激物。

B.23.6 優勢與限制

優勢包括：

- 潛行分析有利於鑑別設計錯誤。
- 當其與危害與可操作性研究(HAZOP)連結應用時效果最佳。
- 極有利於處理具有多重狀態的系統，如批次處理與半批次處理工廠。

限制可能包括。

- 此過程依其應用於電力路徑、製程工廠、機械設備或軟體，而有某些不同。
- 此方法依賴建立正確的網狀樹。

B.24 馬可夫(Markov)分析

B.24.1 一般

馬可夫分析用於系統的未來狀態僅視其目前的狀態而定，通常用以分析可能存在多種狀態之可修復系統，且此系統並不適合使用可靠度方塊分析作充分分析。本方法可使用更高階的馬可夫過程予以延伸至更複雜系統，而僅受模組、數學計算及假設限制。

馬可夫分析過程為一定量技術，且可為不連續的(使用狀態間變化的機率)或連續性的(使用跨越狀態的變化之速率)。

雖然馬可夫分析可以人工運算，然而此技術之本質適合使用電腦程式，市場上即有許多適用之軟體。

B.24.2 應用

馬可夫分析技術可用於各種可修復或不可修復之系統架構，包括：

- 並聯的獨立分項。
- 串聯的獨立分項。
- 負載分擔系統。
- 備用支援系統，包括可能發生轉換失效之情況。
- 劣化的系統。

馬可夫分析技術亦可用以計算可用性，包含考量用於修復時的備用分項。

B.24.3 輸入

馬可夫分析主要的輸入如下。

- 其中所包括系統、次系統或分項的狀態清單[如完全運作、部分運作(即劣化狀態)、失效狀態等]。
- 清楚瞭解可能必須予以模式化的轉變。例如，車輛輪胎失效需考慮到備用輪胎之狀態，且因而考慮到檢查頻率。
- 由一狀態至另一狀態的變化率，典型以不連續事件的狀態間變化機率，或連續

事件的失效率(λ)及/或修復率(μ)表示。

B.24.4 過程

馬可夫分析技術圍繞在如〝可用的〞與〝失效的〞等〝狀態〞之中心概念，且此兩種狀態歷經時間之轉移係依據恆定的變化機率。使用隨機轉移機率矩陣來描述狀態逐一間之轉移，使得以計算各種輸出。

為說明馬可夫分析技術，考慮一複雜系統僅能有三種狀態：運作、劣化及失效，分別界定為狀態S1、S2、S3。此系統每日存在於此三種狀態之一，表B.2顯示此系統

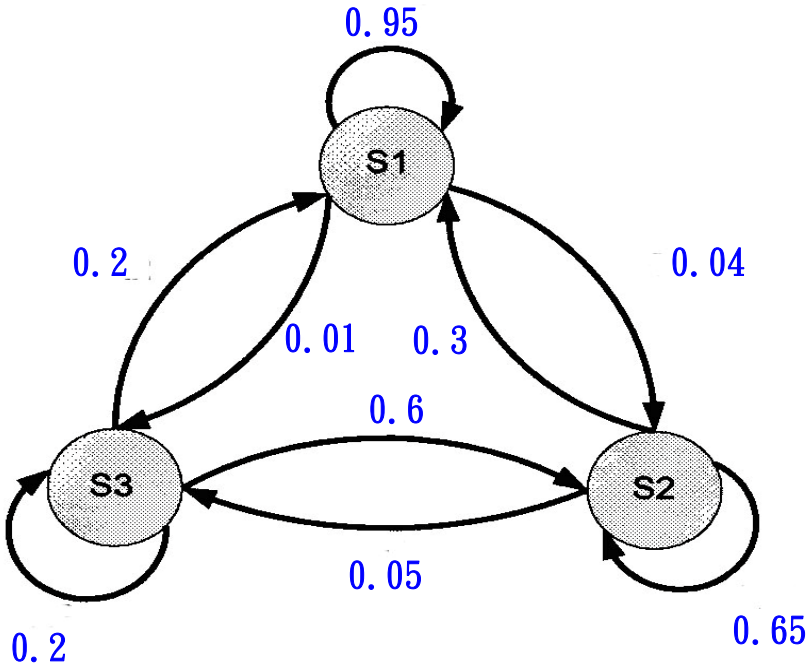
明日在Si(i可為1、2或3)狀態之機率。

表B.2　馬可夫矩陣

		今日狀態		
		S1	S2	S3
明日狀態	S1	0.95	0.3	0.2
	S2	0.04	0.65	0.6
	S3	0.01	0.05	0.2

此機率之陣列稱為馬可夫矩陣，或轉移矩陣。注意到每一欄之總和為1，係每一情況所有可能的結果之總和。此系統亦可以

馬可夫圖表示，圖中之圓圈代表狀態，而箭頭代表轉移及其機率。



圖B.9　系統馬可夫(Markov)圖例

由一狀態回到本身的箭頭通常不顯示，但在此等圖例中為完整之故而予以顯示。

令P*i*表示發現此系統在狀態*i*的機率，*i*＝1, 2, 3，則求解的聯立模擬方程式寫為：

$$P1 = 0.95\ P1 + 0.30\ P2 + 0.20\ P3 \quad \text{(B.1)}$$

$$P2 = 0.04\ P1 + 0.65\ P2 + 0.60\ P3 \quad \text{(B.2)}$$

$$P3 = 0.01\ P1 + 0.05\ P2 + 0.20\ P3 \quad \text{(B.3)}$$

此三個方程式並非獨立的，且將無法解出

三個未知數，須使用下列方程式，並捨棄上列方程式之一。

$$1 = P1 + P2 + P3 \quad (B.4)$$

狀態1，2，3之解答分別為0.85，0.13及0.02。此系統85 %時間完全運作，13 %時間在劣化狀態，而2%時間在失效狀態。

考量兩個並聯運作的項目，要求對此系統之功能係可運作的。此等項目可為運作或失效的，且此系統之可用性係依據項目之狀況而定。

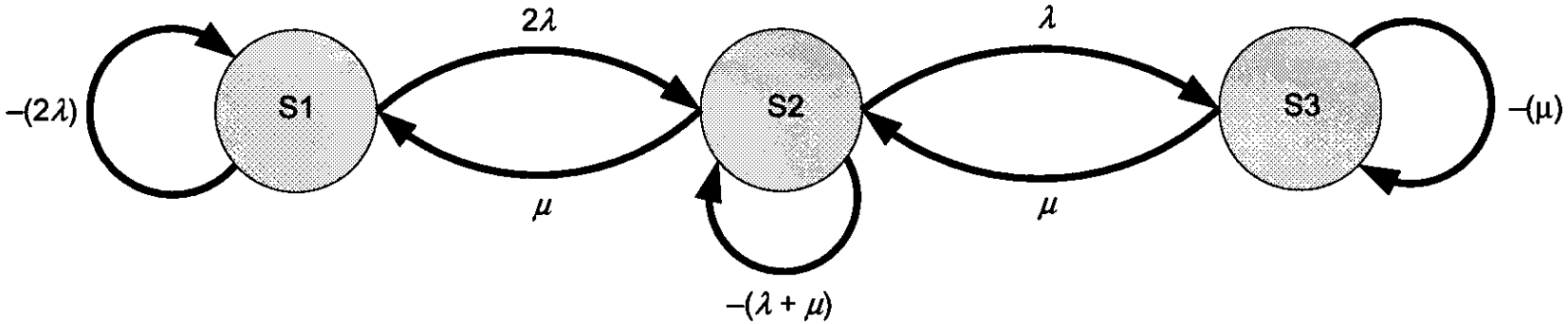
狀態可考量為。

狀態1：兩項目均正確運作。

狀態2：一項目失效且進行修復中，另一項目運作正常。

狀態3：兩項目均失效，惟其一項目進行修復中。

若每一項目之持續失效率假設為λ，惟修復率為μ，則此狀態轉移圖如圖B.10。



圖B.10　狀態轉移圖例

注意到由狀態1轉移至狀態2為2λ，當此兩項目之一失效將導致此系統至狀態2。

令為初始狀態i於時間t之機率。且
令為最終狀態於時間之機率，
轉移機率矩陣形成表B.3。

表B.3　最終馬可夫(Markov)矩陣

		初始狀態		
		$P1(t)$	$P2(t)$	$P3(t)$
最終狀態	$P1(t+\delta t)$	-2λ	μ	0
	$P2(t+\delta t)$	2λ	$-(\lambda+\mu)$	μ
	$P3(t+\delta t)$	0	λ	$-\mu$

值得注意的是0值不可能發生在由狀態1移至狀態3，或由狀態3至狀態1之時，亦且，當指定變化率時，各欄之總和為0。
此模擬方程式成為。

$$dP1/dt = -2\lambda P1(t) + \mu P2(t) \quad \text{.....(B.5)}$$

$$dP2/dt = 2\lambda P1(t) + -(\lambda + \mu)P2(t) + \mu P3(t) \quad \text{.....(B.6)}$$

$$dP3/dt = \lambda P2(t) + -\mu P3(t) \quad \text{.....(B.7)}$$

為簡化由，假設所需之可用性為穩定狀態之可用性。

當趨向於無限值時，將趨向0，而此等方程式形成易於解決，亦須使用上述如方程式

(B.4)所示之附加方程式。

現在，此方程式 $A(t) = P1(t) + P2(t)$ 可表示為。

$$A = P1 + P2$$

因此 $A = (\mu^2 + 2\lambda\mu)/(\mu^2 + 2\lambda\mu + \lambda^2)$

B.24.5 輸出

馬可夫分析的輸出為各種狀態下之各種機率，且因而可估算系統主要分項之一的失效機率及/或可用性。

B.24.6 優勢與限制

馬可夫分析之優勢包括：

- 計算具有修復能力與多劣化狀態的系統機率之能力。

馬可夫分析之限制包括：

- 假設狀態變化的機率為常數，僅限於失效或修復。
- 由於未來狀態除了當前之狀態外，與所有過去狀態無關，故所有事件皆為統計上的獨立事件。
- 需要狀態變化的所有機率之知識。
- 矩陣運作之知識。
- 後果難以與非技術人員溝通。

B.24.7 比較

馬可夫分析類似Petri-Net(派翠網路)分析，均可監測與觀察系統狀態，有些不同係

因Petri-Net(派翠網路)可在同時存在於多狀態中 。

B.24.8 參考文件

IEC 61078 Analysis techniques for dependability - Reliability block diagram and boolean methods

IEC 61165 Application of Markov techniques

ISO/IEC 15909 (All parts) Software and systems enigineering - High-level Petri nets

B.25 蒙地卡羅模擬分析

B.25.1 一般

在使用分析技術予以模式化時，許多系統因不確定性之效應而過於複雜，但其可藉由考慮將輸入作為隨機變數予以評估，並藉由取樣輸入進行N次的數值計算(通稱為模擬)，以獲得希望的結果之N種可能結果。

此方法可處理以分析方法將極難以瞭解與解決的複雜情況。系統可使用試算表與其他傳統工具予以展開，然而更精巧的工具現已易於取得，可協助更複雜的要求，

許多工具在現今已相對地不再昂貴。當初發展此技術時，蒙地卡羅模擬所需的反覆運算次數使該過程緩慢而耗時，然而電腦的進步與理論性的進展，如拉丁超方塊抽樣(Latin-hypercube sampling)，使許多的應用之處理時間幾乎不顯著。

B.25.2 應用

蒙地卡羅模擬提供工具以評估在廣泛的範圍情況中，不確定性對系統的效應。其典型上用以評估可能的後果範圍，以及在此範圍的數值之相對頻率，以定量量測系統諸如成本、期間、加工能力、需求及類似

量測等。蒙地卡羅模擬可用於兩不同目的。

- 傳統的分析模式不確定性之散播。
- 分析技術無效時以機率模式計算。

B.25.3輸入

蒙地卡羅模擬之輸入為系統之有效模式與有關輸入類型、欲表示的不確定性的緣由之資訊及所需的輸出。附有不確定性之輸入資料以分配之隨機變數表示，其或多或少依據不確定度分散。經常為此目的使用均勻、三角、常態及對數常態分配。

B.25.4 過程

此過程如下：

(a)界定模式或演繹計算法，儘可能地近似於代表研究中的系統之行為。

(b)模式使用隨機數字產生此模式的輸出(系統之模擬)並運作多次，如應用上為使不確定性之效應模式化，此模式為提供輸入參數與輸出的關係之方程式形式。選定的輸入值係由代表此等參數中不確定性特性的適當機率分配中取得。

(c)在任一情況中，電腦以不同的輸入運作此模式多次(通常高達10,000次)，並產

生多個輸出。這些可使用傳統統計法予以處理，以提供諸如平均值、標準差、
信賴區間等資訊。
模擬例如下。
考量的案例為兩個同時運作的項目，且系統運作僅需一個項目，第一個項目可靠度為0.9，另一個為0.8。
可依下列各欄建構一試算表。

表B.4　蒙地卡羅模擬例

模擬數	項目1		項目2		系統
	隨機數	運作？	隨機數	運作？	
1	0.577243	是	0.059355	是	1
2	0.746909	是	0.311324	是	1
3	0.541728	是	0.919765	否	1
4	0.423274	是	0.643514	是	1
5	0.917776	否	0.539349	是	1
6	0.994043	否	0.972506	否	0
7	0.082574	是	0.950241	否	1
8	0.661418	是	0.919868	否	1
9	0.213376	是	0.367555	是	1
10	0.565657	是	0.119215	是	1

隨機數產生器產生0與1間之數字，用以與每一項目之可靠度相比較，以決定系統是否運作。如僅作10回合之模擬，所獲得0.9之結果值不應視為正確結果。通常的方式為鍵入計算機，以與模擬進行的總結相比較，以得到所需的準確度。在此例中，經20,000次反復後得到0.9799之結果值。

上述模式可以數種方式予以延伸。例如：

- 延伸模式本身(如考量僅當第一項目失效時，第二項目才立即運作)。
- 當機率無法準確界定時，改變固定機率

為變動機率(良好之例為三角分配)。

- 使用失效率結合隨機數產生器產生失效時間(冪數、韋氏或其他適當的分配)並建構於修復時間內。

在眾多的應用中，其中包括財務預測、投資績效、專案成本/時程預測、業務過程中斷及人員需求等之不確定性評鑑。

分析技術無法提供相關結果或當輸入與輸出資料中具有不確定性時。

B.25.5 輸出

輸出可能為如上例所測得之單一數值，其可能為以機率或頻率分配表示的結果，或

其可能為模式內對輸出具有最大衝擊的主要效應之鑑定。

一般而言，蒙地卡羅模擬將用以評鑑可能產生的結果之整體分配，或分配之重要量測值，諸如：

- 產生界定的結果所產生之機率。
- 問題遭遇者具有某程度的信賴區間，對於結果值將不致超過或予超越，例如成本之變化不超過10 %或耐久期間80 %肯定將超過預期的耐久期間。

分析輸入與輸出間之關聯性，可明顯化進行中的因素之相對顯著性，並鑑別致力於

影響結果不確定性有效的標的。

B.25.6 優勢與限制

蒙地卡羅模擬之優勢包括下列：

- 原則上此方法可適度輸入變數中之任何分配，包括觀察相關系統導出試驗得出之分配。
- 模式發展相對簡單且當需求產生時可予以延伸。
- 實際產生的任何影響或關係可予以呈現，包括諸如狀況可恃性之微妙效應。
- 可應用敏感度分析來鑑別強烈與微弱之影響。

- 輸入與輸出間之關係顯而易見，模式易於瞭解。
- 可利用有效能的行為模式諸如Petri Nets(派翠網路)(IEC 62551)，其經證實對蒙地卡羅模擬極為有效。
- 提供結果的準確度之量測。
- 軟體易於取得且相對而言並不昂貴。

限制如下列：

- 解決方案的準確度依據可執行的模擬數而定(此限制因電腦速度的增進已經變得不重要)。
- 其依賴足以表示參數中的不確定性之有

效分配。

- 大型而複雜的模式可能對訂定模式者為一挑戰，且使難以將利害相關者納入於此過程中。
- 此技術可能不足以衡量高後果/低機率之事件，且因而使組織的風險需求無法反映於分析中。

B.25.7 參考文件

IEC 61649 Weibull analysis

IEC 62551 Analysis techniques for dependability – Petri net techniques

ISO/IEC Guide 98-3：2008 Uncertainty

measurement – Part 3: Guide to the of uncertainty in measurement (GUM:1995)

B.26 貝氏統計法(Bayesian statistics)與貝氏網路(Bayes Nets)

B.26.1 一般

貝氏統計法歸功於Thomas Bayes，其前提是任何已知的資訊(先驗者)可與後續的量測(後驗者)結合建立整體機率，貝氏理論之一般表示法可以下式表示：

式中，X之機率表示為$P(X)$，X在Y已發生的條件下之機率表示為$P(X|Y)$，及Ei為第i件事件。

其最簡化程式可縮減為。

貝氏統計法與古典統計法之不同點在於其並不假設所有分配參數為固定的，而參數是隨機變數。貝氏機率若考量為人員在某一事件的信任程度可更容易瞭解，其與依據實質證據的古典統計學是相對立的。因貝氏法係依據機率的主觀闡釋，其提供決策思維與貝氏網路(或信任網、信任聯結網或貝氏聯結網)的發展之現成基礎。

貝氏網使用圖形模式表示一組變數與其機率的關係，此網路係包含數個表示隨機變數的結點以及聯結母源結點至子結點的箭頭所組成(此母結點為一變數，其直接影響另一(子)變數)。

B.26.2 應用

近年來，貝氏理論與貝氏網路之應用已普及，部分原因為其直覺的魅力，及亦因可取得軟體計算工具。貝氏網路業已應用在廣泛範圍的主題：醫療診斷、影像模組、遺傳基因學、語言辨識、經濟學、太空探險及現今使用最有效的網路搜尋引擎中。

當在任何領域需要透過結構化的關係與數據之利用來找尋散佈各處的未知變數時，，貝氏理論與貝氏網路係有價值的。貝氏網路可用以學習因果關係，提供有關問題領域之瞭解，並預測介入後的結果。

B.26.3 輸入

輸入類似蒙地卡羅模式之輸入，對於貝氏網路，採取的步驟範例包括下列：

- 界定系統變數。
- 界定變數間之因果關係。
- 規定條件機率與先驗機率。
- 附加證據至網路。

- 進行信任之更新。
- 獲取後驗信任。

B.26.4 過程

貝氏理論可以廣泛地應用於各種方式，以下範例將考量使用醫療檢驗決定病患是否患病所建立的貝氏表，進行此檢驗前認為群體99 %的人未患病，1 %的人患病，此即為先驗(Prior)資訊。此檢驗之準確度顯示出若此人患有此病，檢驗結果之期間98 %為陽性的，而且若該人未患病之機率，檢驗結果之期間10 %為陽性的，貝氏表提供下列資訊

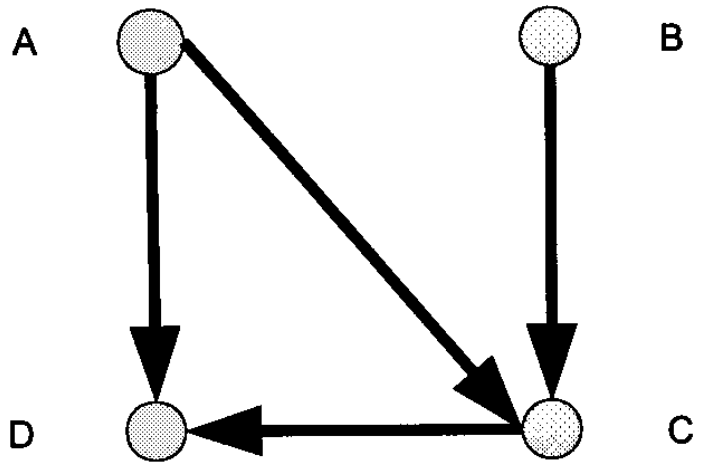
表B.5　貝氏表數據

	先驗	條件機率	乘積	後驗
患病	0.01	0.98	0.0098	0.0901
未患病	0.99	0.10	0.0990	0.9099
合計	1		0.1088	1

使用貝氏法則，乘積由先驗與機率組合決定，由乘積值除以乘積合計值得到後驗值，其產出顯示為陽性的檢驗結果指示先驗由1 %增至9 %。更重要的是，縱使陽性

的試驗，仍有很大機會可能未罹患此病。檢查此方程式(0.01×0.98)/[(0.01×0.98)＋(0.99×0.1)]顯示〝未患病之陽性結果〞值在後驗值中扮演主要角色。

考量下列的貝氏網路。



圖B.11　樣本貝氏(Bayes´)網圖例

以下列各表界定的範圍之條件先驗機率，並使用標註為：Y表示肯定，N表示否定，肯定可能如上述為〝患病〞，或可能為〝高機率〞，而N可能為〝低機率〞。

表B.6　A結點與B結點已界定之下的先驗機率

P(*A*=*Y*)	P(*A*=*N*)	P(*B*=*Y*)	P(*B*=*N*)
0.9	0.1	0.6	0.4

表B.7　A結點與B結點已界定之下的C結點之條件機率

A	*B*	P(*C*=*Y*)	P(*C*=*N*)
Y	*Y*	0.5	0.5
Y	*N*	0.9	0.1
N	*Y*	0.2	0.8
N	*N*	0.7	0.3

表B.8　A結點與C結點已界定之下的D結點之條件機率

A	*C*	P(*D*=*Y*)	P(*D*=*N*)
Y	*Y*	0.6	0.4
Y	*N*	1.0	0.0
N	*Y*	0.2	0.8
N	*N*	0.6	0.4

決定之後驗機率，首先必須計算。
使用貝氏法則，依下列所示決定出，而最末欄顯示常態化機率，依先前範例導出(數值為修正值)總和為1。

表B.9　D結點與C結點已界定之下的A與B結點之後驗機率

A	B	$\mathrm{P}(D \mid A,C)\mathrm{P}(C \mid A,B)\mathrm{P}(A)\mathrm{P}(B)$	$\mathrm{P}(A,B \mid D=N,C=Y)$
Y	Y	0.4×0.5×0.9×0.6＝0.110	0.4
Y	N	0.4×0.9×0.9×0.4＝0.130	0.48
N	Y	0.8×0.2×0.1×0.6＝0.010	0.04
N	N	0.8×0.7×0.1×0.4＝0.022	0.08

為導出 $\mathrm{P}(A \mid D = N, C = Y)$，需合計所有$B$值：

表B.10　D結點與C結點已界定之下的A結點之後驗機率

$\mathrm{P}(A = Y \mid D = N, C = Y)$	$\mathrm{P}(A = N \mid D = N, C = Y)$
0.88	0.12

此顯示出之先驗機率由0.1增至0.12之後驗機率，僅小變化，另一方面，由0.4變動至0.56，其變化更明顯。

B.26.5 輸出

貝氏法可應用於如同古典統計法具有廣泛輸出範圍的相同範圍，如數據分析導出點估計

與信賴區間，其最近之普及程度係於貝氏網路導出後驗分配。圖示輸出提供易於瞭解之模式，且數據可易於修改以考量參數之關聯性與敏感度。

B.26.6 優勢與限制

優勢如下：

- 僅需知道先驗機率。
- 推論的說明易於瞭解。
- 僅要求依據貝氏法則。
- 其提供問題中使用主觀信念之機制。

限制如下：

- 界定貝氏網路內所有複雜系統之相互作用係錯綜複雜的。
- 貝氏法需要知道通常由專家判斷所提供之大批條件機率的知識，軟體工具僅能提供依據此等假設之答案。

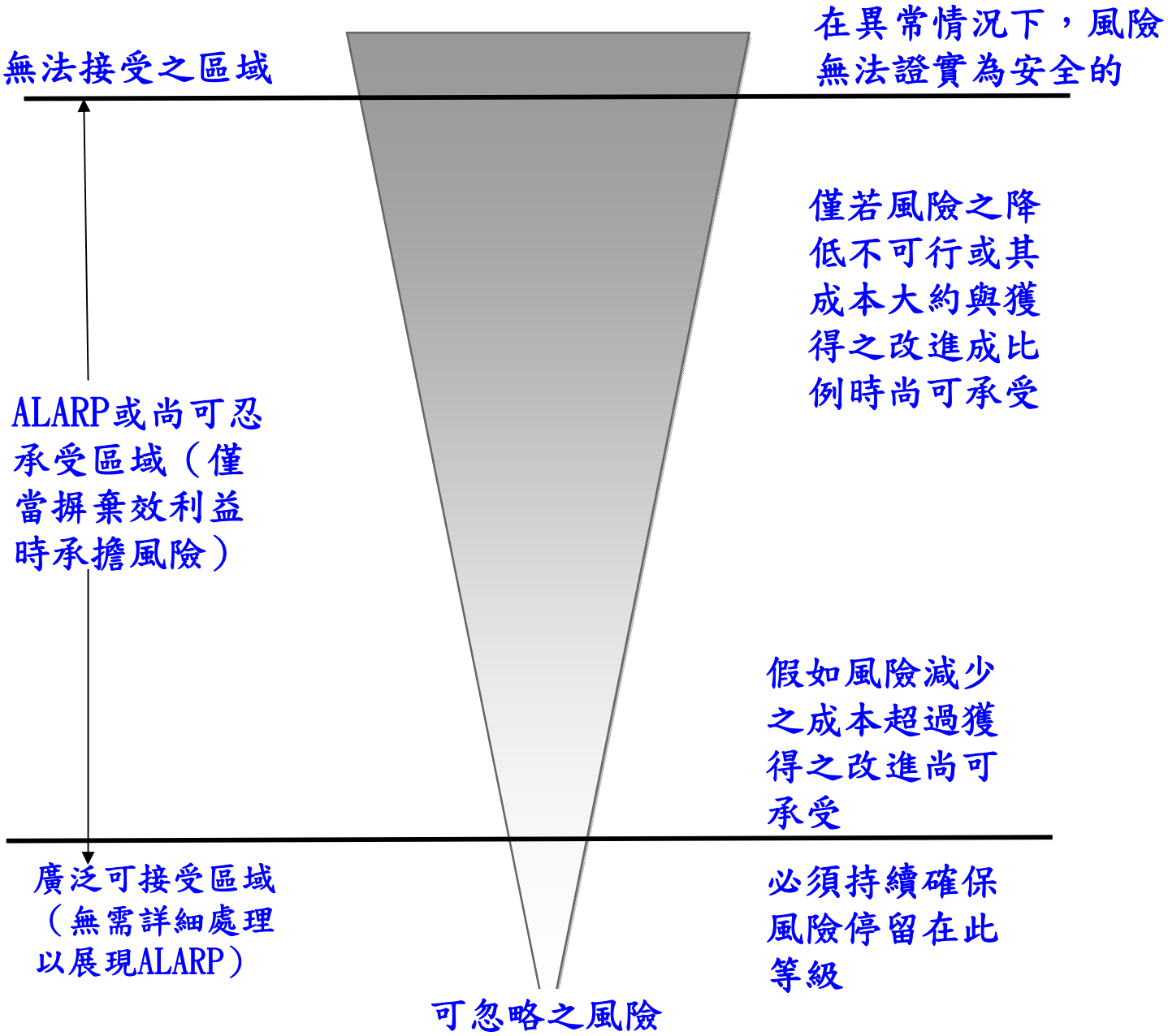
B.27 FN曲線

B.27.1 一般

FN曲線係以圖形表示對特定群體造成特定程度傷害的事件之機率，最通常為提及意外事故發生數目設定之下的頻率。

FN曲線顯示N個或更多群體分項將受到影響

的累積頻率(F)。高N值可能伴隨高頻率F發生，這是重要的關切點，因其可能是社會與政治上無法接受的。



圖B.12　ALARP(最低合理可行原則)概念

B.27.2 應用

FN曲線為一表示風險分析的輸出之方法，許多事件具有高機率的低重要性之後果，以及低機率的高重要性之後果，FN曲線提供風險等級之表示，係以線性描述此範圍，而非以單點表示一項重要性機率之配對。

FN曲線可用以比較風險，例如以界定之準則做出之FN曲線比較預測得知的風險，或是將過去的突發事件之數據，或是和決策準則(亦以FN曲線表示者)比較預測得知的

風險。

FN曲線可用於系統或過程設計，或用於現有系統之管理。

B.27.3 輸入

輸入可為下列之一。

- 在一設定期間內的機率與重要性之配對組。
- 以定量風險分析輸出之數據，估算特定傷亡人數之機率。
- 由過去紀錄與定量風險分析兩者所得之資料。

B.27.4 過程

備妥之資料連同傷亡人數(至一特定傷害等級，即死亡)繪製於圖上，形成橫座標，而以N或更多傷亡人數之機率形成為縱座標，由於數值範圍較大，兩座標軸通常為對數標度。

FN曲線可使用過去耗損之〝真實〞數字以統計方式建構，或可由模擬模式估算值計算出。資料使用及假設設定意味此兩種型式的FN曲線提供不同的資訊，須分別予以使用並用於不同目的。一般而言，理論性

FN曲線對於系統設計最有效，而統計之FN曲線對於特定已有的系統之管理最為有效。

此二導出方式均甚耗時，故使用兩者混合型式並不罕見。然後經驗數據將建構特定期間內已知的意外/偶發事件所肇生確知傷亡事故之固定點，而定量風險分析以外插法或內插法提供其他定點。

考量低頻率、高重要性意外事件的需求可能需要考量長期間，以蒐集適當分析之足夠資料。此可能反倒使備妥的資料因為引發的事件歷經時間變化而引起質疑。

B.27.5 輸出

以線條表現跨越風險後果值的範圍，可用以與適用於該群體與其特定損害程度之準則進行比較。

B.27.6 優勢與限制

FN曲線為表示風險資訊之有效方式，可由管理者與系統設計者用以協助訂定有關風險與安全等級的決策，此手法對於呈現頻率與後果資訊之有效方式。

可取得充分資料時，FN曲線適合於比較來自於類似情況的風險。當資料之量與質

變動之狀況，此方法不適用於比較產生變動的特性之不同型態的風險。

FN曲線之限制為其除受影響人數外，並不說明任何有關事件的效應或後果之範圍，且無法鑑別可能產生的傷害等級之不同方式。其勾劃出通常對人們有害的特殊後果類型。FN曲線並非風險評鑑方法，但為呈現風險評鑑後果的方式之一。

對於呈現風險評鑑後果已有建立的方法，但需要由熟練的分析人員準備，且通常對於非專業人員較難以闡釋與評估。

B.28 風險指數

B.28.1 一般

風險指數為風險之半定量量測，其為以座標標度，使用記分方式導出的估算值。風險指數可用以評定一系列的風險，使用相同準則使其可予以比較。每一風險分項，例如污染物特性(緣由)、可能的暴露途徑之範圍及對感受體之影響等給予記分。

風險指數主要為評定與比較風險之定性方式，當使用數字時，處理上較為簡易。在許多情況中，根本模式或系統並未詳細

瞭解或無法予以表達時，最好使用更完整的定量方式。

B.28.2 應用

若已詳深入瞭解系統，可使用指數來區分與活動相關的不同風險，其使得某範圍對風險等級具有影響之諸因素，整合為風險等級之單一數值分數。

指數用於許多不同類型的風險，通常作為依據風險等級區分風險的訂定範圍之工具，此可用以決定何項風險需進一步深入探討與可能時定量評鑑。

B.28.3 輸入

輸入由系統之分析導出，或情況之廣泛敘述。此需要詳細瞭解所有風險緣由、可能的途徑及何者可能受到影響。可使用如失效(故障)樹分析、事件樹分析及一般決策分析來支援風險指數的發展。

由於座標標度的選擇在某些程度上為隨意的，故需有充分的資料來查證此指數。

B.28.4 過程

首先之步驟為瞭解與敘述此系統，一旦系統經界定後，開發每一分項之多種記分，

使其可予以合計提供合成指數之方式。例如，在環境之情況，緣由、途徑及感受體將予以記分，注意在某些案例中，每一緣由可能有多種途徑及感受體。個別記分依據此系統之實質現況架構予以合計。重要的是每一系統之部分(緣由、途徑及感受體)之記分係內部一致性，並維持其正確關係。可對風險之分項(如機率、暴露、後果)或增加風險之因數給予記分。

記分可依據此高等級模式予以加、減、乘及/或除之，累積效應可考慮增加記分(例如對不同途徑增加記分)。對座標標度應用

數學公式係極為不確實的，因此，一旦記分系統已訂定出，此模式須應用至已知系統方為有效。訂定指數為一反覆的方式，且在分析後果適合查證之前，可嘗試將數種不同系統合併記分。

不確定性可透過敏感度分析說明之，並變動不同記分以找出何項參數最敏感。

B.28.5 輸出

輸出為相對於特定緣由之一系列數值(合成指數)，並可與同一系統內其他緣由產生的指數相比較，或可以相同方式予以模式化

B.28.6 優勢與限制

優勢如下：

- 指數可為提供評定不同的風險之良好工具。
- 其使影響風險等級之多種因素得以整合為風險等級之單一記分數值。

限制如下：

- 若過程(模式)與其輸出未詳細查證，後果可能無意義。以一數值表示風險的輸出，例如在後續的成本/利益分析可能被誤解或誤用。

- 在許多使用指數的情況中，並無基本的模式可界定風險因素之個別標度是否為線性、對數或某種其他形式，且並無模式可界定因數須如何予以合計。在這些情況中，等級在本質上為不可靠的，且依據真實資料查證特別重要。

B.29 後果/機率矩陣

B.29.1 一般

後果/機率矩陣為組合定性或半定量的後果與機率之分級，以產生風險等級或風險分級之方法。

矩陣之格式與其應用之定義依據其使用之情況而定，且對於此情況使用適當的設計係重要的。

B.29.2 應用

後果/機率矩陣在風險等級之基礎上用以排序風險、風險之緣由或風險處理。一般使用為當許多風險業已鑑別之篩選工具，例如，用以界定何項風險需進一步或更詳細的分析，何項風險需優先處理，或何者需提至更高層的管理階層。其亦可用以選擇何項風險在此時不需進一步考慮。此種

風險矩陣亦廣泛用以決定一既定風險，依其在矩陣的定位區域，是否大致上可接受或不可接受(參照5.4)。

後果/機率矩陣亦可用以協助溝通跨組織的定性風險等級之一般性瞭解，風險等級設定之方式與指定的決策規則，須與組織對風險的傾向一致。

後果/機率矩陣之形式可使用於失效模式與效應及關鍵性分析(FMECA)中之關鍵性分析，或於危險與可操作性研究(HAZOP)時設定優先順序。後果/機率矩陣可用於資料不足以充分詳細分析時，或時間與付出不足以

確保更深入的定量分析時。

B.29.3 輸入

過程的輸入為後果與機率依據客製化之標度，以及此兩者組合之矩陣。

後果之標度(或指標)須涵蓋所考量不同類型的後果之範圍(例如財務損失、安全，視情況而定的環境或其他參數)，且須由頂端的可靠後果延伸至關切的最低後果，部分範例如圖B.13所示。

標度可能為任何數字的點，最通常為3、4或5點標度。

機率標度亦可為任何數字之點，機率之界定需儘可能清楚選定，若使用數值指引來界定不同機率時，則須給予單位。機率標度需橫跨目前研究的相關範圍，謹記最低機率必須為頂端界定後果可接受的，其他所有具有頂端後果的活動則界定為不容許的，部分範例如圖B.14所示。

以後果為一軸及機率為另一軸繪出矩陣，圖B.15顯示具有6點後果與5點機率標度的矩陣之部分範例。

指定至格內的風險等級依據機率/後果標度之定義而定。矩陣中可以設定對後果(如

所示者)或機率給予額外的權重，或依據應用給予設定對稱的權重建立。風險等級可聯結至如管理階層注意的程度或回應所需的時間標度之決策規則。

分級	財務衝擊	投資報酬	健康與安全	環境與社會	名聲	法規與符合
6	(數額)利益或損失	(數額)利益或損失	・多重災難或 ・不可逆重大效應作用在若干萬人	・不可逆長期環境傷害 ・社區暴動、政治上長期案件活動	・若干時日的國際性報導 ・完全喪失事件相關者支持並停止投資 ・執行長離職且委員會改組	・重大控訴金額逾伍仟萬，另加上龐大費用 ・公司執行階層受到拘留起訴 ・政府機關延長擱置公司營運
5	(數額)利益或損失	(數額)利益或損失	・單一災難及/或 ・不可逆嚴重損傷在一或數人身體上	・延長的環境衝擊 ・引起社群的高度關切—重覆地發生重大的解決措施……	・若干時日的全國性報導 ・事件相關者名聲的永續性衝擊；事件相關者缺少支持……	・重大控訴金額逾壹仟萬 ・政府機關介入調查使公司業務中斷……
4	(數額)利益或損失	(數額)利益或損失……	不可逆傷害或……	……	……	……
3	(數額)利益或損失	……	……	……	……	……
2	……	……	……	……	……	……
1	……	……	……	……	……	……

圖B.13　後果準則表部分圖例

等級	準則
近似	・機率平衡會發生，或…… ・在數週或數月內會發生……
有可能	・近期內會發生，或…… ・數月內會發生……
不大會	・有機會發生，或…… ・數月後才發生……
甚少	・有發生的機會……
稀少	・理論上會發生……

圖B.14　風險排序矩陣部分圖例

可能性等級							
	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		後果等級					

圖B.15　機率準則矩陣部分圖例

等級標度與矩陣可以定量的標度建立，例如，可靠度情況中，機率標度可表示指示的失效率，而後果標度表示失效之金錢成本。

此工具之使用需要具有相關專業知識的人員(最好為一小組)，且備妥此等資料以協助後果與機率的判斷。

B.29.4 過程

為評定風險，使用者首先尋找最適合此情況的後果敘述，然後界定產生此等後果的機率，風險等級其後可由矩陣讀出。

許多風險事件可能具有不同的相關機率之後果範圍，通常，次要問題較重大災難更為常見，因此得以選擇是否評定最通常的後果，或最嚴重者或某些其他組合。在許多情況中，適合著重於最嚴重之可信後果，因其提供最大的威脅且通常最被關切。在某些情況中，可能適合同時分別評定一般問題與重大災難各別風險。重要的是，使用所選定的後果相關之機率，而非整體事件的機率。

風險等級以矩陣界定出，可能與例如處理或不處理此風險的決策規則有關。

B.29.5 輸出

輸出為每一風險之評定，或以界定的重要性等級之風險排序列表。

B.29.6 優勢與限制

優勢如下：

- 相對易於使用。
- 提供依不同重要性等級之風險迅速排序。

限制如下：

- 須設計適合狀況的矩陣，使其難以具有可跨越相關於組織狀況範圍之共通系統。
- 難以清楚地界定標度。

- 使用上極為主觀性，評定者間易有明顯的差異。
- 風險無法合計(即無法界定特定數量的不同低度風險或已鑑別的單一低度風險發生特定數次後相當於中度風險)。
- 難以合併或比較不同類型的後果之風險等級。

後果依分析的詳細程度而定，即分析得越詳細，越多具有較低機率之情境數，此將低估實際的風險等級。描述風險時集合情境的方式須為一致性的，且在研究開始時即界定。

B.30 成本/效益分析(CBA)

B.30.1 一般

成本/效益分析可用於風險評估，將總成本期望值與總效益期望值相互比較，以選擇最佳或最有利的選項。成本/效益分析是許多風險評估系統中內隱的部分。其可以是定性或定量的，或包含定量或定性要項之組合。定量的成本/效益分析，總計發生在涵蓋範圍內所有利害相關者的所有成本與效益之金錢價值，並按照其不同期間進行調整後累計其成本與效益。如此產生的

淨現值(net present value，NPV)可作為為有關風險決策之輸入值。某一措施可產生正淨現值(NPV)時，通常意指須採取該項措施。然而，在面對某些負面風險時，尤其是涉及對人類生命的風險或對環境的損害者，可應用最低合理可行(ALARP)之原則，將風險區分為三區域：(1)高出此一範圍的負面風險無法接受，除非情況極為特殊；(2)低於此一範圍之風險可以忽略，僅須監測以確保其仍維持在低風險；及(3)一個中階層範圍，其中風險降低到其最低合理可行(ALARP)程度。此區域之朝向低風險端，

可一律應用嚴謹的成本效益分析除非風險接近到無法承受程度時，最低合理可行(ALARP)原則之預期為除非處理之成本與所獲得之效益極不成比例，否則便將予以處理。

B.30.2 應用

成本/效益分析可用於在涉及風險的選項間作成決定。

例如：

- 作為有關一風險是否須予以處理的決策之輸入。

- 區分與決定最適當的風險處理方式。
- 決定不同的措施途徑。

B.30.3 輸入

輸入包括提供給相關利害相關者的成本與效益之資訊，及有關此等成本與效益的不確定性。須考量實質與無形的成本與效益。成本包括所消耗的資源與負面後果，效益包括其正面後果、所可避免的負面後果及所節省的資源。

B.30.4 過程

利害相關者所可能遭受到的成本或收到的

效益皆須鑑別之，在完整的成本效益分析中，所有均包括在內。

鑑別出與所考量選項有關的所有相關利害相關者的直接與間接效益與成本，直接效益是直接來自於所採取的措施者，而間接或附屬效益係碰巧發生的，但可能仍對決策有明顯助益者。間接效益之範例包括商譽改進、員工滿意度及〝心安(peace of mind)〞(這些效益通常在做出決策時給予大的權重)。

直接成本係直接與措施有相關者，間接成本為附加的、輔助的及沈沒成本，如公共

事業之損失、消耗的管理時間或由其他有潛力投資所挪用的資金。當對是否處理風險之決策應用成本效益分析時，須包括與處理此風險及接受此風險有關的成本與效益。

在定量的成本/效益分析中，當所有實質與無形的成本與效益經鑑別後，應確定所有成本與效益(包括無形的成本與效益)的金錢價值。有數種標準方式可用以進行此一步驟，包括〝樂意支付〞方式或使用等值。若類似經常發生的狀況，成本發生於短期間內(如一年)，及效益則持續發生在

往後的一個長期間內，通常必須將此效益折現使其成為〝今天的現金(today's money)〞以便進行一個有效的比較。所有成本與效益均以現值(present value)表示之。所有利害相關者的所有成本與所有效益之現值，可予以總合產生淨現值(NPV)。正淨現值(NPV)意味此措施有益。有關效益成本比率之使用，亦可參照B.30.5。

若有關成本或效益的程度具有不確定性，其任何一項或兩者均可依其機率權重估計之。

在定性的成本效益分析中，並不試圖找出

其無形成本與效益之金錢價值，不但不提供一個成本與效益，定性成本效益分析考量不同成本與效益間之關係與權衡得失(trade-offs)。

成本有效性(cost-effectiveness)分析與此類似，成本有效性分析假設有一期望效益或後果，且有數種達成方式。此分析僅審視最經濟方式達成效益之成本。

B.30.5 輸出

成本/效益分析之輸出為有關不同的選擇或措施相對成本與效益之資訊。此可以

淨現值(NPV)、內部報酬率(internal rate of return，IRR)之淨現值(NPV)，或以效益現值對成本現值之比率定量表示之。此輸出之若以定性表示時，輸入通常為包含不同類型的成本與效益之成本與效益比較表，將注意力集中在權衡得失。

B.30.6 優勢與限制

成本效益分析之優勢為：

- 成本與效益得以使用單一計量(金錢)比較之。
- 提供訂定決策之透明性。

• 需要所有可能的決策事項所蒐集之詳細資訊，此對揭示無知及溝通訊息上可為有價值的。

限制為：

• 在使用不同的方法對非經濟效益指定其經濟價值時，定性成本效益分析可能產生戲劇化的不同數字。

• 在某些應用上，難以界定未來成本與效益正確有據的折現率。

• 難以估計所帶給大眾的效益，尤其與沒有市場交易的公共財有關者。

• 使用折現方法，表示認為未來長期所獲

取的效益將根據所選定的折現率折現，其對於決策的影響微不足道。除非設定極低或接近於零折現率，否則此方法不適用於考量可能影響未來世代的風險。

B.31 多準則決策分析(MCDA)

B.31.1 一般

目標為使用一系列相關判斷標準客觀地與透明地評鑑一組選項之整體價值。一般而言，整體目的是在可用選項間做出優選順序。此分析包含發展出一個經過排序與總計的選項與準則矩陣，用以提供每一選項

之整體記分。

B.31.2 應用

多準則決策分析(MCDA)可用以：

- 比較多個選項以便做首輪合格分析，以決定優選且有潛力之選項，與不適當的選項。
- 比較具有多重性且有時與準則衝突之選項。
- 當不同的利害相關者具有相衝突的目標或價值時，達成有關決策之共識。

B.31.3 輸入

一組分析之選項，依據目標之準則可均等地在所有選項間使用以區分之。

B.31.4 過程

通常由一組知識豐富的利害相關者施行下列過程。

(a)界定目標。

(b)決定有關每一目標之屬性(準則或績效量測)。

(c)將屬性建構於階層中。

(d)依據準則發展欲評估的選項。

(e)決定準則的重要性並分配相當之權重。

(f)評估關於準則之替代選項，此可以記分之矩陣表示。

(g)多個單一屬性之記分加總為單一多屬性記分。

(h)評估後果。

每一準則之權重可依不同的方法導出，且有不同方式將每一選項之準則記分加總為單一多屬性記分，例如，記分可以權重之總和或權重之乘積加總之，或使用分析階層過程，依據成對比較的權重與記分之導出技術。所有此等方法假設任一準則之偏好並不依賴其他準則之數值，當此假設有

誤時，則使用不同的模式。
由於記分為主觀的，敏感度分析有助於檢查權重與記分影響選項間整體偏好之程度。

B.31.5 輸出

評定係由最偏好至最不偏好之順序表示，若過程產生矩陣，其矩陣之軸為每一選項的權重準則與記分準則，則高度不符合的權重準則的選項亦可予以刪除。

B.31.6 優勢與限制

優勢為：

- 提供有效能的決策訂定以及假設與結論

的表示之簡單架構。

- 可作成未能經得起成本/效益分析的複雜性決策問題，更易於處理。
- 可協助理性地考量需要考量其間權衡得失的問題。
- 當利害相關者具有不同的目標及其準則時，可協助達成協議。

限制為：

- 可能受到決策準則之偏差與不良選擇之影響。
- 大部分的多準則決策分析(MCDA)問題並不具有包羅廣泛或唯一的解決方案。

- 由陳述的偏好計算權重準則演算法加總，或加總不同的意見，可能模糊決策的真正基礎。

參考資料

[1] CNS 22000 食品安全管理系統－食品供應鏈中組織之要求

[2] IEC 60300-3-11 Dependability management – Part 3-11: Application guide – Reliability centred maintenance

[3] IEC 61078 Analysis technique for dependability - Reliability block diagram and boolean methods
[4] IEC 61165 Application of Markov techniques
[5] IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems
[6] IEC 61511 Functional safety - Safety instrumented systems for the

process industry sector
[7] IEC 61649 Weibull analysis
[8] IEC 61882 Hazard and operability studies (HAZOP studies) - Application guide
[9] IEC 62551 Analysis techniques for dependability - Petri net techniques
[10] ISO/IEC 15909 (all parts) Software and systems engineering - High-level Petri nets
[11] ISO/IEC Guide 51 Safety aspects - Guidelines for their

inclusion in Standards

相對應國際標準

IEC/ISO 31010:2009 Risk management – Risk management techniques