IOSH安全資料表　機械設備危害評估方法　類號：SDS-C-007

總號：0082

介紹

1. 使用範圍

機械設備風險評估主要目的在於從機械設備的設計階段即將危害因子納入考量，並設法消除，因此風險評估是消除危害，保障安全的第一步。風險評估必須至少考量設計意圖(Design Intention，含機械設計範圍)、危害因子鑑別(Hazard Identification)、危害偵測(Hazard Detection)及安全保護(Safety Protection)等層面。

2. 名詞解釋

(1) 安全對策：消除危害或是降低風險的方法。

(2) 殘餘風險：實施安全對策之後仍然存在的風險。

(3) 可預見的：在合理的範圍內，依據學理、習慣、現況等，可推算或預測的結果。

(4) 傷害：物理性受傷和/或對健康的損害，或對財務的損壞。

3. 使用場所(作業)、行業、職種、相關作業環境

風險評估有定性評估、半定量評估和定量評估法，有由上而下的(Top Down Assessment)，也有由下而上的(Bottom Up Assessment)。對於任何一個問題，必須考量事件的特性及大小、嚴重程度、發生頻率、影響程度、可取得的資訊、可投入的資源……等因素，決定所要採用的評估方式。原則上沒有最完美的評估方法，只有最恰當的評估方法。

使用

1. 機械設備風險評估是以一連串具有邏輯的步驟，並以系統性的方法，檢視機械設備相關危害的作法。通常機械設備風險評估之後，緊接著進行危害消除。當此程序重復的進行時，即成爲儘可能消除機械設備相關危害的閉迴路循環系統，進而增進機械設備的安全性。

2. 風險評估通常包括風險分析和風險評量兩部份；其中風險分析包括：決定機械設備的使用限制、危害因子鑑別和風險估算。危害消除雖然緊接著風險評估之後進行，但不屬於風險評估的一部份。風險評估的流程可以用下圖表示：

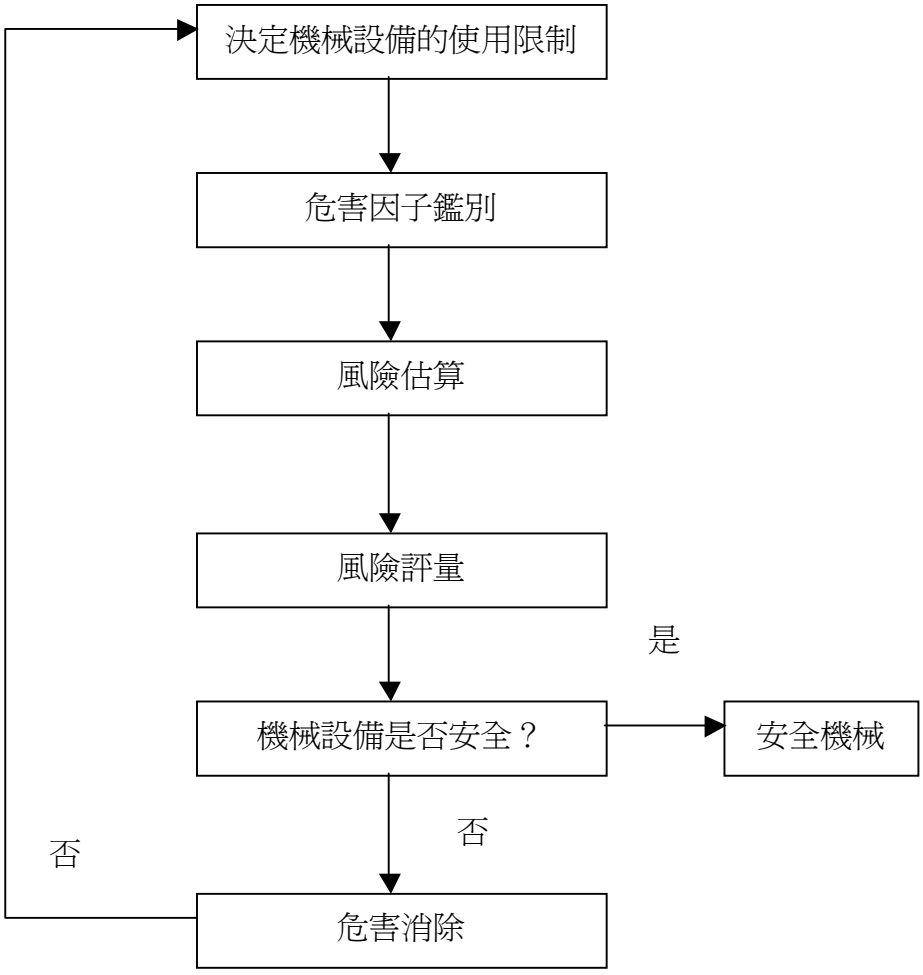

圖1　機械設備風險評估的流程

3. 進行風險評估時，必須依據學理和事實做合理的判斷與決定。此判斷和決定必須以定性法或定量法爲依據，並儘可能使用定量法進行，尤其是可預見危害的傷害及嚴重性很高時，更應使用定量法。然而實際進行風險評估時，由於資料數據的限制，通常無法進行定量評估，只能使用定性評估。

4. 定量法同時可評估各種不同的安全對策和方法，並決定何者的安全防護性最佳。

5. 進行風險評估(不論使用定性法或定量法)時，必須充分的收集資料，這些資料最少應包括：

   (1) 機械設備的使用限制

   (2) 機械設備生命週期各階段的需求

   (3) 設計圖或其他任何形式足以表明機械本質的資料

   (4) 機械動力源的資料

(5) 此類型(甚至相似類型)機械設備曾發生意外事故的資料

(6) 對健康造成傷害的任何資料

上述資料在設計的過程中或是進行修改後，應隨時更新以保持資料的正確性。

6. 若是缺乏此類型機械設備的意外事故的記錄，或是甚少發生意外事故，或是意外事故的嚴重性很低，都不可以自行假設此機械設備的風險很低。

7. 進行定量評估時，可使用資料庫、手冊、實驗室中的數據，和製造商所提供的規格和數據，但是這些數據必須具有公信力或是被工程界所認可的。若是這些數據具有不確定性，則應在評估過程中加以說明。

8. 進行風險評估時應至少考量下列因素：

(1) 機械設備生命週期的各個層面

(2) 機械設備的使用限制，包括使用範圍與方式(正確的使用方式和合理可預見範圍之內的誤用或機械故障)

(3) 機械在所有範圍內可預見的使用包括工業用、非工業用或家庭用；可能的使用者的性別、年齡、慣用左/右手和生理能力的障礙，如體型、體力、視障或聽障等

(4) 可預見使用者的能力、經驗和接受訓練的程度，如操作者(包括受過訓練的維修人員及技術人員)、正在受訓的學員、生手或是一般大眾

(5) 可預見的範圍內其他人員可能曝露在機械設備的危害下

9. 所有與機械設備有關的危害因子、危害條件與狀態和危害事故都應加以鑑別。

10. 當各項危害因子都已鑑別時，即可針對各別的危害因子進行風險估算。

11. 風險是危害發生可能性與危害發生後嚴重性的函數，即

風險＝f(危害發生的可能性，危害發生後的嚴重性)。

12. 危害發生的可能性通常由下列三項因素決定：

(1) 人員曝露在此危害下的頻率和時間

(2) 發生危害事故的可能性

(3) 避免或限制危害發生的技術及人為因素，如降低操作速度、緊急停機裝置、警告標示和訊息、人員操作狀態和注意力、訓練程度等

13. 上述考量通常無法準確的定義，只能大致估算，尤其是對危害發生的可能性。有時危害發生後的嚴重性也無法計算，例如因爲毒性物質或生理壓力造成人員的健康危害等。

14. 計算危害發生後的嚴重性時，應考量下列各項因素：

(1) 防護的對象

A. 人員

B. 機械設備或財物

C. 環境

D. 生產停頓

(2) 對健康造成危害的嚴重性

A. 輕微的(通常是可復原的)

B. 嚴重的(通常是不可復原的)

C. 死亡

(3) 影響的範圍

A. 一人

B. 多人

(4) 財物損失

A. 單機

B. 多機

C. 生產線

D. 全廠

E. 容易修復

F. 不容易修復

(5) 環境影響

A. 廠內

B. 擴散至廠外

C. 容易清除

D. 不容易清除

(6) 生產停頓

A. 數小時

B. 數天

其他的影響因素如環境清除費用、居民圍廠、商譽損失、停工待料損失等，可以在評估的過程中考量是否加入考量。

15. 計算曝露的頻率和時間，應考量下列因素：

(1) 進入危險區域的必要性，包括正常操作、維修或修理時

(2) 自動或手動進退料

(3) 持續進入危險區域的時間

(4) 需要進入危險區域的人數

(5) 進入危險區域的頻率

16. 計算發生危害事件的可能性，應考量下列因素：

(1) 機械設備和其元件的可靠度或其他的統計數據

(2) 發生意外事故的歷史記錄

(3) 對健康危害的歷史記錄

(4) 與類似機械設備風險的相對比較

(5) 監測系統與保護系統的完整性，如互鎖裝置等

17. 計算避免或限制危害發生的可能性，應考量下列因素：

(1) 機械設備的操作者

A. 有經驗及技巧的技術人員

B. 無經驗或技巧的人員

C. 無人操作(自動化操作)

(2) 危害事件發生的速度

A. 突然發生

B. 很快的發生

C. 很慢的發生

(3) 風險的警告訊息

A. 一般警告訊息

B. 直接觀察

C. 由警告標示和警報裝置提供

(4) 人員的反應以避免或限制危害發生的可能性(如反射行爲、快速逃離等)

A. 可能

B. 在適當的條件下可能

C. 不可能

(5) 對機械設備的知識或實務經驗

A. 有經驗

B. 對類似的機械設備有經驗

C. 沒有經驗

18. 估算風險時應對每項危害因子，考量下列項目：
    (1) 曝露的人員，包括操作員及其他可能受到影響的人員
    (2) 曝露的型式、頻率和時間
    (3) 曝露與危害影響之間的關係
    (4) 人因/人體工學，如人機介面、人與人的反應、生理/心理狀態、對危險的反應等
    (5) 安全功能的可靠度，考量各種安全功能的效果(最好用定量法)，並決定最佳的安全防護對策及方式。
    (6) 避開或破壞安全防護功能的可能性，此項因素與安全防護的型式及其設計息息相關。
    (7) 繼續維持安全防護能力的可能性。

19. 執行風險估算之後，即進入風險評量階段，以決定機械是否已達到安全的要求，或是尚未達到安全的要求，而必須進行危害消除。如果必須進行危害消除，則必須選擇和應用適當的安全對策，並重復進行上述的風險評估。另一方面也需要注意，不可因爲增加安全對策，而引發二次危害，同時也應將此項納入風險評估的範圍內。

20. 常用的風險分析的方法有：
    (1) 假如分析法(What-If Analysis)
    (2) 查核表(Checklist Analysis)
    (3) 危害與可操作性分析(Hazard and Operability Analysis)
    (4) 失誤樹分析法(Fault Tree Analysis)
    (5) 事件樹分析法(Event Tree Analysis)
    (6) 失效模式和影響(和關鍵性)分析法【Failure Mode, Effects(and Criticality)Analysis】

    這些方法中包括了定性分析法和定量分析法，有些分析方法如FTA、ETA和FMECA可適用於定性和定量分析方式，甚至適用於半定量分析法；然而有些分析方式如What-If和Checklist多使用在定性分析方面。一般而言，定性分析所使用的人力、經費、時間和資源較少，相對的所得到的結果較不完整和深入。定量分析可得到完整而深入的量化結果，可提供決策者充實的資料與數據，做爲政策決定的判斷依據，然而相對的，所投入的人力、經費、時間和資源也需要相對的增加。決定使用定性或是定量分析方法的依據，在於可投入的人力、時

間和相關的資源與系統的危害度和關鍵程度。若是系統的危害度和關鍵程序都很高，則應實施定量分析法。反之，定性分析法即已足夠提供所需的資訊了。同樣的這些分析方法中有的是由下而上的(Bottom-Up Analysis)如FMECA等，有些是由上而下的(Top-Down Analysis)如FTA、ETA等。這兩種方式各有其優點與缺點，端視系統的特性和預期分析的結果，決定使用的分析方法。必須說明的是，沒有任何一種分析方法可以適用於所有的系統與狀況；同時沒有最好的分析方法，只有最恰當的分析方法，端視系統的特性、操作/使用的狀態、預期分析的目的……等因素而定。

21. 假如分析法：此種分析方式是最簡單，也最經濟的分析方法。其做法是將系統(或次系統、子系統)內可能發生的危害情況列出，接著決定這些危害可能產生的影響及其嚴重程度，系統內是否有適當且足夠的保護裝置或措施，訂定對系統現況的改善建議或應採取的行動。簡易的"假如分析表"可採用下表中的格式：

表一：假如分析表格式

系統名稱：

日期：　　分析負責人：

假如	影響/嚴重度	保護裝置/措施	改善建議/行動

假如分析法的成敗取決於參與分析的人員與其專業性，因此參與分析的成員非常重要。成員不但要具備足夠的專業知識和能力，同時要對分析對象的操作、使用、維修、安裝等狀況充分了解，才能夠進行有意的分析。另一方面分析負責人不但需要確認成員的能力，也必須確認成員的廣度，足以包括分析對象所有的層面，這樣才能確保分析的完整性，否則很容易發生遺漏。同時分析負責人的整合能力及專業素養也是決定分析結果與品質的重要關鍵。此分析法的優點是簡單、快速、投入的資源較節省。而其缺點爲分析結果取決於分析負責人和成員、分析的結構性不夠嚴謹、結果無法量化、分析完整性不足等。

22. 查核表：

查核表的分析方式，通常也是應用在定性分析時使用。其優點與缺點和假如分析法類似，其作法爲將系統內可能發生的所有危害，以查核表的方式列出，並根據這些危害發生的機率，發生後的嚴重度，決定

此項危害的風險值。同時由系統內的保護裝置，隔離裝置和偵測裝置等決定是否足以減少危害發生的機率或降低危害的影響，從而決定是否需要進行改善。若是系統過於複雜，則可將系統分爲數個次系統，以方便分析的進行。常見的查核表分析法可用下表的格式進行分析。

表二：查核表分析格式(以機械式動力衝床爲例)

飛輪區					
項目	危害發生機率	影響嚴重度	風險值	保護裝置	建議/行動
飛輪捲入	5	3	15	已加裝護罩	無
旋轉棒打擊	1	5	5	加裝護蓋	無
……	……	……	……	……	……
操作區					
項目	危害發生機率	影響嚴重度	風險值	保護裝置	建議/行動
無雙手按鈕	2	4	8	設置雙手按鈕	雙手按鈕應具備同時性
無按鈕盒	2	3	6	無	裝按鈕盒
……	……	……	……	……	……
電氣區					
項目	危害發生機率	影響嚴重度	風險值	保護裝置	建議/行動
電線絕緣破壞	3	5	15	無	加強檢查與更換
電線跳接	5	4	20	無	禁止跳接

註：a. 危害發生機率分爲5級，極可能爲5，有可能爲4，可能爲3，不太可能爲2，極不可能爲1。

b. 影響嚴重度分爲5級，災難性爲5，很嚴重爲4，嚴重爲3，不太嚴重爲2，不嚴重爲1。

c. 風險值=危害發生機率x影響嚴重度

查核表分析法的成功與否，和查核表的優劣直接相關。完整且語意清楚的查核表可以很容易的帶領分析人員一步一步的執行分析作業；相反的，若是查核表內容不夠完整，會使得分析結果發生疏漏，造成決策中心的錯誤判斷；而語意不清的查核表會使得分析人員在使用時不知所云，造成分析時的困擾。另一方面分析負責人和分析人員的專業能力當然也是此分析方法成功的關鍵因素。必須注意的是不同的系統需使用不同的查核表，甚至同樣的系統在不同的操作條件或是操作環境之下，查核的內容也不相同，因此在製作或選用查核表時，需要特別的謹慎和小心。事實上沒有任何一種查核表是可以適用於所有的系統的，同時系統的變異性很大，因此較佳的方式是針對各種系統可能有的特性，如機械、電氣、互鎖、控制、化學、自動化……等，分別製作查核表(這些查核表的範例將在下一章說明)。進行分析時則選用

適當的部份加以組合應用，以符合實際的需要。必須注意的是這些查核表的內容是依據一般系統常見的項目加以製作，並不代表其完整性，因此使用者在使用這些查核表時必須根據分析系統的特殊需求，增減查核表的內容。這也同時說明了分析負責人與分析人員專業能力重要性的原因。

23. 危害與可操作性分析：

危害與可操作性分析是常見的較爲詳細的分析方法，可應用在定性和定量的分析。危害與可操作性分析的作法是將系統分爲一系列的節點，並將系統的設計基線作爲參數(這些參數可以是流量、溫度、壓力、液位、濃度、容量等)，再將偏離設計基線的狀況用引導語(如高、低、無、反向、錯誤等)來表示，從而推論出導致這些偏離狀態的原因，可能引起的影響，系統內的保護裝置或措施是否足夠，進而訂定改善措施或行動，以達到保障人員與設備安全的目的。進行危害與可操作性分析時首先需決定節點，通常是將系統內對特定適用的參數及其產生的影響相類似的一部份劃分爲同一節點，如在儲存區內可以將一個儲槽，其連結的幫浦和連結的管線，當做一個節點。必須注意的是在進行分析時若發現同一節點可能導致不同的影響時，應將該節點的分析範圍再確定，不可混淆或模糊。如發生洩漏時，洩漏到排水管線和洩漏到環境土壤內是不同的影響，此時應將此節點的分析範圍確定爲排水管線或是環境土壤，以便繼續進行分析。執行危害與可操作性分析時可採用下表的格式：

系統名稱：

節點編號：

日期：

參數	引導語	偏離	可能原因	影響	保護裝置	建議/行動
流量	高	高流量	幫浦異常	無安全顧慮	無	無
壓力	低	低壓	壓力源異常	機器停止	禁止啓動	無
溫度	高	高溫	加熱器過熱	火災	警報器	加裝滅火設備
轉速	高	高轉速	電源異常	機器損壞	過電流保護器	加裝漏電斷路器
方向	錯誤	流向錯誤	逆止閥失效	化學品混合引起反應	無	加裝互鎖裝置
流量	無	無流量	幫浦失效	無法冷卻系統過熱	溫度感測器	加裝互鎖開關
……	……	……	……	……	……	……

上述的作法爲定性的危害與可操作性分析，若加入偏離的發生頻率和影響嚴重度，則此分析方法亦可應用於定量分析。

24. 失誤樹分析法：

失誤樹分析法是從系統的失效現象做出發，再根據這些失效現象，配合系統的作動原理，操作條件，操作環境等因素，分析失效發生的原因及造成系統失效的可能部位，失效後的影響，系統內的偵測裝置、隔離裝置、保護裝置是否足夠，從而決定是否需要進行系統的安全改善。在執行FTA時可將系統失效現象不斷向下展開，直到無法繼續展開爲止。

對系統進行FTA分析時包括下列步驟：

(1) 分析並掌握實施FTA對象的作動原理、操作環境、操作條件和設計功能等基本資料。

(2) 確定系統的頂層事件

(3) 分析頂層事件的次一層要件，並將這些要件以邏輯符號連結之。

(4) 對各項次層要件，分析其更次層要件，並以邏輯符號連結。

(5) 重複(4)的分析直到底層要件(基礎階層)爲止。

(6) 檢討FTA結果，提出改善建議。

現以離心式泵浦作爲FTA分析的範例，其步驟如下：

A. 掌握設備的基本資料

此步驟是執行FTA分析的先決條件，若是無法確實掌握設備的作動原理、設計功能、操作條件、操作環境和操作狀態等基本資料，在進行FTA時，就無法使用充足的資訊，對事件進行展開，使FTA的結果不確實。尤其重要的是在進行定量FTA時一定要有足夠的失效率數據，否則將無法量化頂層事件，也無法據以提出改善意見。本例中離心式泵浦是在常溫常壓下，將弱酸性(PH=5)物質，經由管線送往儲槽中。馬達爲三相220伏特，轉速1750RPM，其額定揚程爲10米水柱。

B. 確定系統的頂層事件

系統的頂層事件多以系統的失效現象爲主，本例中離心式泵浦的頂層事件計有泵浦無法揚水，水量不足揚程不足，軸承損壞，軸承壽命短，聯軸器損壞，泵浦振動噪音大，主軸彎曲，迫緊填料摩耗大，壓力表指示不當和馬達過負荷等十餘項。根據這些頂層事件再做次層要件的展開。

C. 分析次層要件並將這些要件與上層事件以邏輯符號連結

次層要件是造成上層事件的原因，這些原因各自獨立。由於一

個或多個次層要件無法發揮設計的功能，才會造成上層事件的發生。至於次層要件與上層事件之間的關係，則以邏輯符號表示，例如OR Gate ，AND Gate…等。

離心式泵浦的FTA分析項目很多，現舉一例說明。在泵浦啓動後即失水的失效現象中，即以此失效現象爲頂層事件，而會造成此失效現象計有泵浦灌水不足，吸入口吸入空氣，吸入口高於原先設計和吸入口出現空氣袋等四種原因。其中泵浦灌水不足和吸入口高於原先設計已是底層要件，無法再繼續展開。但是吸入口吸入空氣則可繼續展開成進水口與吸入口太接和底閥位置太淺形成水渦等兩項次層要件(此例中亦爲底層要件)。而吸入口出現空氣袋亦可繼續展開到配管不當的次層要件。而這些要件皆各自獨立，且任何一項要件的發生都會造成上層事件的發生，因此這些要件皆須以OR Gate來連結。

D. 檢討FTA結果，並提出改善意見

檢討FTA的頂層事件，以確定這些頂層事件是否能接受，若是不能接受頂層事件，則針對各項次層要件擬定改善措施，以避免頂層事件的發生。

上述即爲簡易型的FTA定性分析的步驟，也是定性的失誤樹分析法。事實上在完成各項要件與上層事件之FTA分析之後，必須對各次層要件賦予失效機率，並根據這些機率計算上層事件和頂層事件的發生機率，最後判斷頂層事件的機率是否可接受。若無法接受則針對關鍵性或高失效率的底層要件，進行改善措施。

25 失效模式和影響(和關鍵性)分析法：

失效模式和影響(和關鍵性)分析法是以系統無法達到其所設計的功能爲理念，從系統內的最小零組件爲分析起點，評估系統內零組件發生失效時對系統所產生的影響。

對系統進行FMEA分析時，需包含下列步驟：

(1) 界定系統，次系統或組件等的功能。

(2) 決定實施FMEA的基礎階層。

(3) 確認系統內各項功能機制，並以方塊圖表示。

(4) 確認各功能失效模式，失效原因與失效效應。

(5) 界定失效影響，檢測失效的方式和建議的處置措施。

(6) 對於高失效率或高失效影響的基礎階層，檢討改善措施。

參考資料

1. 系統分析方法。
2. EN1050 Safety of Machinery---Principles for Risk Assessment
3. EN292-1:1991 Safety of machinery - Basic concepts, general principles for design - Part 1: Basic terminology, methodology
4. EN292-2:1991 Safety of machinery - Basic concepts, general principles for design - Part 2: Technical principles and specifications
5. EN60204-1:1992 Safety of machinery - Electrical equipment of machines - Part 1: General requirements
6. CEN/CLC Memorandum No.9:1994 Guidelines for the inclusion of safety aspects in standards
7. IEC 812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
8. IEC 1025 Fault tree analysis (FTA)