Bureau of Standards, Metrology and Inspection

經濟部標準檢驗局 103 年度

自行研究計畫 103BSMI-13

電器商品事故鑑定調查方法之研析

-以開飲機為例

經濟部標準檢驗局臺中分局　編印

中華民國 103 年 12 月 20 日

本報告書僅供政府機關參考，請勿轉載

標準檢驗局臺中分局 103 年度自行研究計畫			填表人：李政哲 填表日期：1031130
研究報告名稱	電器商品事故鑑定調查方法之研析-以開飲機為例		
研究單位 及研究人員	臺中分局(第一課) 李政哲、蕭景文	研究 期程	自 103 年 1 月 1 日 至 103 年 12 月 10 日
報　　告　　內　　容　　提　　要			

壹、研究緣起與目的

鑑於消費者家中的開飲機於現實生活中時常發生自燃事件，進而造成消費者身家財產傷害，因此開飲機這種產品實為一安全風險性極高之商品。為了解目前市售開飲機之安全性，特別以本安全性分析，針對事故發生原因進行模擬再現試驗及相關改進措施，

貳、研究方法與過程

以市售開飲機(隨機選取)來進行拆解、組件分析，燃燒試驗等加以測試，以安全性分析方式將所有可能造成燃燒事故的組件及因素列舉出呈現。

參、研究發現與建議

目前針對市面上之事故產品，標準檢驗局之作法為再行取樣或購樣以相關標準進行安規測試，惟該作法無法識別有關產品材質結構老化造成事故因素，因此在事故產品分析中應加入安全性分析，藉以將相關建議有效的回饋到安全性驗證系統。

至於其他屏蔽方式的開發，仍可依事故產品發生的型態，對應其問題設計開發，期望能夠將事故發生率降至最低，有效保障生命財產安全。

目錄

頁次

表目錄

頁次

圖目錄

頁次

第一章 緒論

1.1 研究背景與動機

隨著社會經濟的不斷發展，小型飲水機已普遍使用於賓館、學校、家庭，給人們的生活帶來了極大的便利，其潛在的火災隱患也時刻危及人們的消防安全。另外，鑑於消費者家中的開飲機於現實生活中時常發生自燃事件，進而造成消費者身家財產傷害，因此開飲機這種產品實為一安全風險性極高之商品。為了解目前市售開飲機之安全性，特別以本安全性調查針對事故發生原因進行探討分析及相關改進措施，首先蒐集該產品發生燃燒事故時之相關資料，並與轄區廠商討論產品設計方向，最後希望藉由燃燒試驗來得知事故發生的原因為何？此為本安全性調查所要掌握及進行的方向。

在此過程中，將屏除以國家標準檢驗方式來進行研究分析，但仍會秉持國家標準條文適用原則來強化事故原因分析之符合性。對於造成火災事故之產品在此計畫中將有更深層次的瞭解，全面向的剖析，應用點線面的概念從小處開始著手進而推敲出產品之風險性程度，並可在火災事故調查處理中協助火災原因之鑑定。

1.2 研究方法與步驟

研究方法將針對燃燒進行定義及介紹，接著以市售開飲機(隨機選取)來進行拆解、組件分析，燃燒試驗等加以測試，以全面性探討方式將所有可能造成燃燒事故的組件及因素列舉出呈現。

首先，在電性領域的認知，實務上涉及火災事故的飲水機，其本身主要是依靠電能進入發熱元件中來提升發熱組件的溫度，使得開飲機可以初步將熱水膽由室溫開始加熱，達到設定工作溫度後經由溫度

開關將電能輸入脫離，如此為一循環為該產品的運轉特性。

接著要了解產品設計結構及採用組件之成分與規格，是分析認定原因的基礎。其動作工作原理情況是什麼?在設計方面是否存在注重使用功能、而忽視安全性能的問題，都需要逐一分析。

其中，溫控裝置正常運行是確保飲水機安全運行的機制，與發熱元件相鄰的部件是否為易燃材料?亦或以阻燃材料進行處理，能否符合防火安全要求?這種情況下，其相關保護組件一旦發生故障，極易強迫著火於相鄰的可燃部件而引發火災。

另外，即使產品無任何故障，是否有可能經由外力或外物入侵造成產品火災事故，也是本計劃研究的方向之一。

1.3 研究貢獻

提取物證是電氣火災原因認定正確的重要階段。火災物證分析是對火災現場勘查中發現並收集的各種痕跡物證的審查、分析、核對總和鑒定，其目的是根據這種物證的本質特徵，分析它的形成條件及與火災過程的聯繫，從而確定其對火災原因的證明程度。

然而在此產品事故安全性調查中，由於消費者發生起火事故時，如果損害不大通常會直接將產品丟棄或是逕洽廠商討論賠償事宜，假使影響層面較大時或一般將由消防局介入處理，此時依法令規定該證物將入消防局存放集調查，檢驗局通常無足夠的物證可供分析研究。

因此，究其困境，本調查內容以對產品檢驗的經驗，分類市面上開飲機的使用結構，交叉分析早期產品與近期改良產品之組件差異性，全面性跳脫國家標準檢驗項目的框架進行調查。因為產品檢驗僅以新品為測試物件，檢驗合格不代表產品百分之百就不會發生事故，仍須考量組件老化、外力影響等因素，期望本調查之內容可提供業者

及民眾對於設計製造開飲機產品及使用開飲機產品上有更進一步的認知。

1.4 研究架構

第一章為緒論，概要說明本研究之相關背景。

第二章為安全性量測之介紹，引入新的安全觀念，其中包含了：安全相對性、安全貫穿系統的整個壽命期間、危險源是事故發生的根本原因、系統可靠性和安全性相輔相成。

第三章為安全性分析之介紹，為提高其安全性，應在產品的研發階段，通過系統化、規範化的分析、設計、驗證等工程活動，預防災難事故損失，降低使用風險，提高產品使用效能，期望使用科學的分析與其數據來完成安全性分析，進而可獲得改進的方案。

第四章承前兩章所說明的安全性量測、要求及其分析，可將其理論架構實際上的運用在事故風險較高的開飲機之產品上，期望透過這些理論的有效運作，能夠找出導致危害的原因，進而可提出修正的建議可用以回饋於安全性設計上的考量。如此一來，安全性設計即可透過修正之設計理念來消除和控制各種危險，提高產品的安全性。

第五章為本研究之安全性調查結論與建議，期望藉此能夠將事故發生率降至最低，有效保障生命財產安全。

第二章 安全性量測介紹

2.1 前言

安全是伴隨人類發展的永遠主題，但是在不同的時期，我們所要面對的安全問題有很大的不同。早期人們所面臨的安全問題相對簡單，主要表現在自然災害和人為災害。隨著科學技術的不斷進步，我們在利用技術推動社會進步的同時也伴隨著新的問題。

為了解決複雜系統的整體性和安全性問題而開發安全性工程理論和方法系統。可在系統壽命期間內應用系統工程和管理方法，辨識系統中的危險源，並採取控制措施使其危險性最小，然後讓系統在規定的性能、時間和成本範圍內達到最佳的安全程度。

安全系統創新了新的安全觀念，其中包含了：安全相對性、安全貫穿系統的整個壽命期間、危險源是事故發生的根本原因、系統可靠性和安全性相輔相成。系統安全注重整個系統壽命期間的事故預防，尤其強調在新系統的設計開發階段採取措施來有效的消除及控制危險源。

2.2 安全性量測

安全性一般用事故發生機率與嚴重程度來評估，目前常用的有事故率／機率、安全可靠度、損失率／機率、事故風險等，最終歸納為事故風險來綜合評估。

2.2.1 事故率或事故機率

事故率或事故機率（Accident Rate or Accident Probability）是安

全性的一種基本參數。其量測方法為在規定的條件下和規定的時間內，系統的事故總次數與壽命單位總數之比，即 $P_A = N_A / N_T$ 其中：P_A 為事故率或事故機率，次／單位時間或百分比（%）；N_A 為事故總次數，包括由於裝備或設備故障、人力因素及環境因素等造成的事故總次數；N_T 為壽命單位總數，表示裝備總使用持續時間的量測，如工作小時、飛行小時、飛行次數、工作循環次數等。

當壽命單位總數 N_T 用時同，如飛行小時、工作小時表示時，P_A 稱為事故率；當 N_A 用次數，如飛行次數、工作循環次數等表示時，P_A 稱為事故機率

2.2.2 安全可靠度

安全可靠度（Safely Reliability）是與安全有關的安全性參數。其量測方法為在規定的條件下和規定的時同內，在裝備執行任務近程不發生由於設備或零件故障造成的災難性事故的概率，即 $R_S = N_W / N_{T2}$ 其中：R_S 為安全可靠度，百分比（%）；N_W 為不發生由於裝各裝備各故障造成災難性事故的次數；N_{T2} 為用使用次數、工作循環次數等表示的壽命單位總數。

2.2.3 損失率或損失機率

損失率或損失概率（Loss Rate or Loss Probability）是安全性的一種基本參數。其測量方法為在規定的條件下和規定的時同內，系統的災難性事故總次數與壽命單位總數之比，即 $P_L = N_L / N_T$ 其中：P_L 為損失率或損失機率、次／單位時間或百分比（%）；N_T 為由於系統或設備故障造成的災難性事故總次數；N_T 為壽命單位總數，表示系統總使用持續時間的測量，如工作小時、工作次數、工作循環次數等。

當壽命單位 N_T 用時間、工作小時表示時，P_L 稱為損失率；當 N_T 用次數、工作循環次數等表示時，P_L 稱為損失機率。損失機率為 $P_L = 1 - R_S$ 其中 R_S 為安全可靠度（%）。

2.2.4 事故風險評估

事故風險評估是國內外最為常用的安全性量測方法，美國、英國和澳大利亞、NASA 和 ESA 等均應用事故風險來量測安全性，美國最近使用 GEIA-STD-0010 事故風險評估。

事故嚴重性等級劃分：事故的嚴重性對由人為失誤、環境條件、設計缺失、系統、子系統或設備故障等引起的事故後果規定了定性的要求；一般分為四級：災難性（I）、嚴重（II）、輕度（III）和輕微(IV)，如表 2-1 所示。對具體的系統來說，事故嚴重性等級的劃分應由訂買方和製造方共同訂定。

表 2-1 事故嚴重性等級劃分

等級	嚴重性	事故後果
I	災難性	人員死亡、裝備毀壞、不可能恢復的環境嚴重損害
II	嚴重	人員嚴重受傷、裝備嚴重毀壞、可恢復的環境嚴重損害
III	輕度	人員輕度受傷、裝備輕度毀壞、可恢復的環境輕度損害
IV	輕微	輕於 III 等人員受傷、裝備毀壞或環境損害

事故可能性等級劃分由人為失誤、環境條件、設計缺失、系統、子系統或設備故障等引起的事故可能性規定了要求，一般分為 5 級：頻繁(A)、很可能(B)、有時(C)、極少(D)、不可能(E)，如表 2-2 所示。事故可能性等級劃分上，不同的標準亦可能不同。

表 2-2 事故頻率等級劃分

等級	發生程度	產品個體	產品總體	機率範圍
A	頻繁	壽命期內可能經常發生	連續發生	$P > 10^{-2}$
B	很可能	壽命期內可能發生幾次	經常發生	$10^{-4} < P < 10^{-1}$
C	有時	壽命期內有時會發生	發生幾次	$10^{-5} < P < 10^{-4}$
D	極少	不易發生，但壽命期內可能會發生	極少發生，預期可能發生	$10^{-6} < P < 10^{-5}$
E	不可能	很不容易發生，在壽命期內可能不發生	極少發生，幾乎不可能發生	$P < 10^{-6}$

因此可使用定性的方法對安全性進行量測。安全性定量的量測，可以用事故率/事故機率、安全可靠度、損失率/損失機率，但此三項量測模式均可納入事故風險量測的範疇，更全面、細緻的量測，可應用定量的事故風險量測。

定量的事故風險量測是在事故嚴重性等級劃分的基礎上，給出每一各級別的具體機率要求或統計各嚴重等級機率。如事故率/事故機率的量測本質上是各級別機率的總合。在具體型號中，可根據產品的需求和實際情況而定。

2.3 安全性量測之功能性

(一)有效地預防事故和減少損失

預防事故、減少損失是安全性工程的主要目標，全面地展開安全

性工程工作，識別系統中存在的薄弱環節和可能導致事故發生的條件，通過系統分析來找出導致事故發生的真正原因，特別是可以分析出未知的、易被忽視的危險因素，並且通過數據分析，預測事故發生的可能性及後果的嚴重性，從而可以採取相應的措施，來預防及控制事故的發生。

(二)用最少投資達到最佳的的安全效果

對系統的安全性進行數據分析，優化系統的安全性設計，為安全管理和事故預防提供科學依據。根據分析可以選擇出最佳方案，使各個分系統之間達到最佳配合，用最少的投貢得到最佳的安全效果，從而可以最大可能地避免事故來降低損失。

(三)迅速提高設備研發人員的安全技術水平

通過系統化地實施安全性工程，不僅可以提高安全技術人員的專業水平，還能使設備系統的設計和使用維修人員了解掌握各種系統分析及評估方法，提高安全技術人員、人員和管理人員的業務水平和系統分析能力，以便能夠很好地提高整個設備的安全水平，預防事故的發生。

(四)系統地進行安全管理

安全性工程通過系統分析、評估，全面系統地、預防性地處理設備中的安全問題，而不是孤立地、就事論事地去解決安全問題，實現系統安全管理。

(五)促進各項安全性標準制定和數據累積

安全性工程的一項重要工作就是要對設備的安全性做出定性或定量評估，這就需要有各項安全性標準和數據，如可接收的最低安全風

險，人機工程設計要求和安全性設計準則等。因此，安全性工程工作可以促進各項安全性標準的制定和有關安全性數據的收集，為建立安全性數據庫打下基礎。

2.4 安全性量測概念與定義

(一)安全-SAFE

不發生可能造成人員傷亡、職業病、設備損壞、財產損失或環境損害的狀態。該定義是指產品壽命周期所處予的狀態，包括試驗、生產和使用等，指產品在某一時刻安全與否的狀態。

(二)安全性- SAFETY

產品所具有的不導致人員傷亡、系統毀壞、重大財產損失或不危及人員健康如環境的能力。

安全性是各類設備的一種相關性的固有屬性，與可靠性、維修性和保障性等密切相關，是各種設備必須滿足的首要設計要求，是通過設計賦予的設備屬性。

(三)軟體安全性-SOFTWARE SAFETY

軟件具有的不導致事故發生的能力。

(四)危險-HAZARD

可能導致事故的狀態或情況，危險是事故發生的前提或條件，可以用危險模式或危險場景來表達。

(五)事故- MISHAP

造成人員傷亡、職業病、設備損壞、財產損失或環境破壞的一個或一系列意外事件。事故描述已經發生的事件，也是危險導致的結果。

(六)事故可能性- MISHAP PRIBABILITY

特定事故發生的可能程度，一般用機率計算或可能性等級來描述。

(七)事故嚴重性-MISHAP SEVERITY

事故發生後果的嚴重程度，一般用嚴重等級來描述。

(八)事故風險-MISHAP RISK

事故嚴重程度和發生機率的綜合量測。

2.5 危險源與分類

危險是由多種不確定因素共同造成的，為了便予分析研究危險的來源，在工程上引入了危險源的概念，用予表明引發危險的根本原因。

設備中的危險源直接或間接威脅著人員，裝備本身以及周圍環境，它們來自周圍環境(如工作環境、自然環境)，系統或設備的工作特性及工作需要(如含有有毒、可燃、輻射、能源等危險品)和人的自身行為(設計、制造、試驗等)。它們均是一種潛在的敘險，在一定條件下將引發事故。為此，必須充分認識和理解各種危險源，以便在設計中進行分析，制定和實施有效的控制措施，從而保障設備的全性。

2.5.1 依危險產生的來源分類

危險產生的來源主要有四個方面:

(一)產品自牧固有的危險特性(如能量或毒性)

(二)產品(硬體或軟體)

(三)人為差錯(包括由心理、生理等因素所引起的行為失誤)

(四)有害的環境

構成產品自身危險的主要來源:產口或產品使用的材料中固有危險；設計缺陷; 制造缺陷。一般而言，設計問題可能是其中最重要的方面。設計人員不僅可能在設計產品時，引入了設計缺陷，造成產品自身的危險，還有可能缺乏正確控制產品及其材料中危險的能力。製造缺陷一般由不正確的生產品質所造成，但在某些忮況下，設計人員也對製造缺陷負有責任。

在產品使用和維修過程中，人為疏失也是造成危險的重要原因。例如，操作中按錯開關，維修時接插件錯誤連接，都可能造成嚴重後果。。除此之外，會對安全產生直接影響的設備故障及有害壞境也是造成危險的不容忽視的因素。例如，飛行過程中發功機空中停機是一項很可能會造成機毀人亡的危險。很多自然壞境和不良的工作壞境都可能造成災維性後果，如雷擊、龍捲風、地震、酸雨；密閉空同中的高溫、高濕壞境等。

2.5.2 依在事故中所起的作用分類

根據能量意外釋放而言，事故是能量或危險物質的意外釋放，作用於人體或設備的過量能量以及干擾人體與外界能量交換的危險物質是造成人員傷害的直接原因。因此，把系統中存在的、可能發生意外釋放的能量或危險物質在這邊歸類為第一類危險源。第一類危險源的存在是導致事故發生的根本原因，它決定了事故後果的嚴重程度。第一類危險源越多，事故的嚴重程度就越高。

在產品使用和使用過程中，為了利用能量，讓能量按照我們的想法在產品中運行，必須採取措施約束、限制能量，用以必控制危險源。理論上說，約束、限制能量的遮罩裝置應該可靠的控制能量，防止能量意外釋放。實際上，絕對可靠的控制措施並不存在。在許多因素的複雜作用下，約束、限制能量的控制措施亦有失效的可能，能量遮罩可能被破壞而發生事故。導致約束、限制能量措施失效或破壞的各種不安全因素和為第二類危險源。從系統安全的觀點來考量，使能量或危險物質的約束、限制措施失效，破壞的原因因素，即第二類危險源，包括人、機、壞境三個方面的向題。第二類危險源往往是一些圍繞第一類危險源隨時發生的現象，是導致事故發生的直接原因，決定了事故發生的可能性。第二類危險源出現得越頻繁，發生事故的可能性越大。

在第二類危險源中，人的因素是指人的不安全行為，即人為疏失。人為疏失可能直接破壞對第一類危險源的控制，造成能量或危險物質的意外釋放。人為疏失也可能造成產品的故障，產品的故障進而導致事故。例如在新品組裝時的失誤，或是維修時未依原廠設計規格來進行維修。

機的因素主要是指產品故障，故障可能直接使約束、限制能量或危險物質的措施失效而發生事故。例如，電線絕緣損壞發生漏電；管路破裂使其中的有毒有害介質洩漏等。有時一個產品的故障可能導致另一另產品的故障，最終造成事故。產品的故障有時會誘發人為疏失，人為疏失也可能會造成產品的故障，最終導致事故。

壞境因素主要指系統運作的壞境，包括溫度、濕度、照明、粉塵、通風換氣、噪音和振動等物理壞境。不良的物理環境會引起產品的故

障或人為疏失。例如，潮濕的壞境會加速金屬腐蝕而降低結構或強度；工作場所強烈的噪音影響人的情緒，分散人的注意力而發生人為疏失。導致事故的發生是兩類危險源共同起作用的結果，如圖 2-1 所示。第一類危險源的存在是事故發生的前提，沒有第一類危險源就談不上能量或危險物質的意外釋放，也就無所謂事故。另一方面，如果沒有第二類危險源破壞對第一類危險源影響，也不會發生能量或危險物質的意外釋放。第二類危險源的出現是第一類危險源導致事故的必要條件。第二類危險源的主要表現形式，是圍繞第一類危險源互生的隨機現象，動態預防性管理的重點。

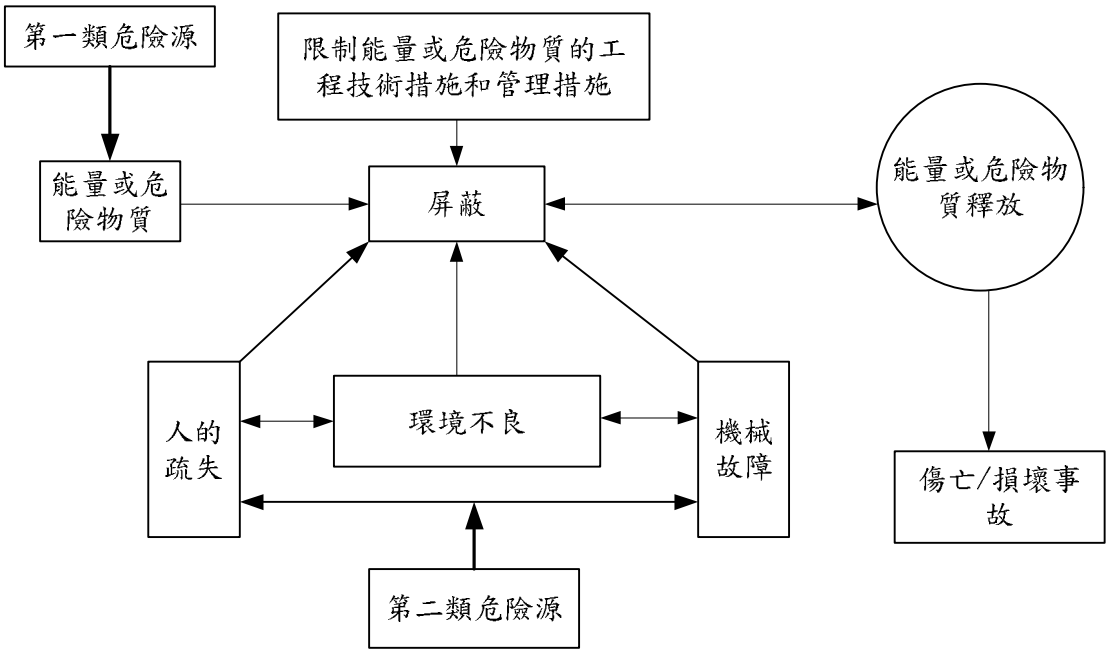


圖 2-1 危險源及事故關係

2.5.3 常見危險源

識別系統中的危險源是提升安全性分析，提出安全性措施的前提和基礎。產品中或多或少都存在著危險源，任何一個部件或一種行為在特定的時間或空間裡都有可能造成不良後果，構成危險狀態。GJB /Z99-1997 中按照物理現象對危險源進行了分類，共分為 15 類危險，

如表 2-3 所列。

表 2-3 常見危險源

序號	危險種類	危險來源	序號	危險種類	危險來源
1	環境危險	自然環境和誘發環境	9	材質變異	腐蝕、耐久應力、老化、疲勞
2	熱	冷、熱、溫度變化	10	著火	燃料、氧化劑、點火源
3	壓力	氣壓、液壓	11	爆炸	物理爆炸、化學爆炸
4	毒性	刺激、窒息	12	電氣	電擊、起火、熱量、靜電
5	震動	高頻、低頻、震動傳輸	13	加速度	加速、減速、衝擊
6	噪音	普通噪音、爆炸	14	機械	擠壓、咬合、碰撞、撞擊、夾斷、剪切
7	輻射	游離輻射、非游離輻射	15	污染	雜質、黴菌、化合
8	化學反應	腐蝕、分解			

2.6 安全性一般要求

安全性要求是安全性工程中展開設計、分析、驗證與評估等工作的依據，正確且科學地確定各項安全性要求是一項重要工作。

安全性要求包括定性要求和定量要求，定性要求指的是用一種非量化的形式來描述對產品安全性的要求；定量要求採用安全性參數、指標來規定對產品安全性的要求。此外，為了保障安全性工作在系統中能夠順利地運作。

安全性要求的制定應具有系統性和完整性。要求應保證能夠識別和處理系統在使用壽命內的所有危險，並確保這些危險被正確消除，

或這些危險帶來的風險在可接受的範圍內。制定安全性要求的目的就是要在產品研發中，通過設計分析驗證與評價和管理等工作，使事故風險在可接受范圍內。

安全性要求制定方式依據設備的壽命與任務目的，掌握安全性制定的總體考量和關鍵要素，科學合理的制定既滿足安全性需求，又符合實際設計、生產水平與使用保障條件等約束條件，與設備研發的其他要求綜合技術，達到最佳的使用效能。同時，研發人員只有在充分理解這些要求後，才能將安全性正確地設計到產品中去，並有計劃地實施有關的組織、監督和控制工作。

2.4.1 安全性要求

安全性定性要求一般包括：安全性措施優先次序要求；安全性具體設計要求；安全性定性風險評估要求；安全性信息要求。

(一)安全性措施的一般優先次序要求一般從風險的角度來看，設備安全性遵從以下的設計原則。

(1) 消除危險：安全性工程中，首先應盡量採取可行的措施將危險消除，可以從系統結構設計、安全性設計技術以及使用特性設計等方面採取措施。所採取的安全性措施必須與工程周期，費用和技術水平等進行考量，並滿足用戶的安全性要求。

(2) 減輕危險影響：若某危險或相關的危險模式不能被徹底消除，那麼要盡量減這些危險帶來的可能事故影響。可通過設計方案的選擇、降低發生概率和採取保護措施等技術將其減少到消費者方可接受水平。

(3) 控制危險：對於不能消除的危險，除了通過保護措施降低危

險影響外，還須要對在系統使用過程中殘餘的危險進行控制。這些控制措施在系統設計階段就應納入安全性工程的工作。

控制危險的措施及優先順序如下：

(1) 採用安全裝置：若不能通過設計消除已判定的危險或不能通過設計方案的選擇滿足消費者方的要求，則應採用永久性的、自動的或其他安全防護裝置，使風險降低到消費者方可接受水準。

(2) 採用警報裝置：若不能和安全裝置都不能有效地消除已判定的危險或滿足消費者方的要求。則應採用警報裝置來檢測出危險狀況，並向有關人員發出適當的警報信息。警報信息應明顯，以盡量減少人員對信號做出錯誤反應的可能性。

(3) 制定特定程序和進行培訓:若通過設計方案的選擇不能消除危險，或採用安全裝置和警報裝置也不能解決，則應制定特定程序安全程程序及緊急備案等，並進行培訓。

(二)安全性定性設計要求

安全性定性設計要求一般包括以下幾個方面

(1) 減少危險品要求：設計人員通過設計、選材等方法，盡量減少或取消系統對危險品的使用，或將危險品相關事故風險降低到可接受的範圍。

(2) 危險品隔離要求：將危險物品、危險元器件和危險操作與其他人員、活動、區域和不相容的器材相隔離。

(3) 設備安置要求：設備安置應使得在對其使用、維修過程中人員盡量避免暴露於危險（包括危險物、高壓電、電磁輻射和切割、衝擊物等）。

(4) 安全保護要求：採用機械隔離或屏蔽的方法保護系統的能量源、控制裝置和關鍵零組件。

(5) 安全設備要求：定期對用於減少風險的相關安全設備（如互鎖裝置、消防器材等）進行功能檢查

(6) 報廢處理要求：在系統設計階段需要考慮保證系統報廢處置的安全。

(7) 警告信號要求：警告信號的設計應保證盡量減少人員對該類信號的漏判和誤判，警告信號要與相似系統具有一定的通用性。

(8) 警告標誌要求：當不能通過設計消除危險時，應在裝配、使用、維護說明書中發出警告和注意事項，並在危險零部件、器材、設備和設施上標出醒目的標記，以使人員、設備得到保護。

(9) 人員技能要求：參與安全關鍵的任務時，要求參與人員具有較高的技能。因此，在設計階段要提出相關的人員技能審定要求與過程。

(10) 風險最小化要求：設計的系統在各種約束條件下，達到人員傷亡、設備損壞和環境破壞的風險最小化。

安全性設計工作初期，應在分析和審查有關標準、規範、條例、設計手冊等的適用性之基礎上，結合產品的實際情況和以往的經驗分

析、特殊危險分析等確定安全性設計要求。

第三章 安全性分析

3.1 前言

為了提高產品的安全性，應在其研發階段，通過系統化、規範化的分析、設計、驗證等工程活動，預防災難事故損失，降低使用風險，提高產品使用效能，期望使用科學的分析與其數據來完成安全性分析，進而可獲得改進的方案。

3.2 安全性分析的目的和作用

安全性分析、設計和驗證等工作的流程如圖 3-1 所示。安全性分析也可以稱為危險分析，它是安全性工程的核心內容，包括危險的識別與其理論分析、風險分析與評估等，是安全性設計、評估的基礎。安全性分析是通過對系統進行深入地分析，檢查系統或設備在每種使用模式中的工作狀態，確定潛在的危險，預計這些危險會對人員傷害、設備損壞或環境破壞的嚴重性和可能性，為確定消除或減少危險的方法(包括改進系統設計或改變系統運作流程)提供依據，以便能夠避免事故的發生，或者盡量減少事故發生的可能性或降低事故有害影響的程度。

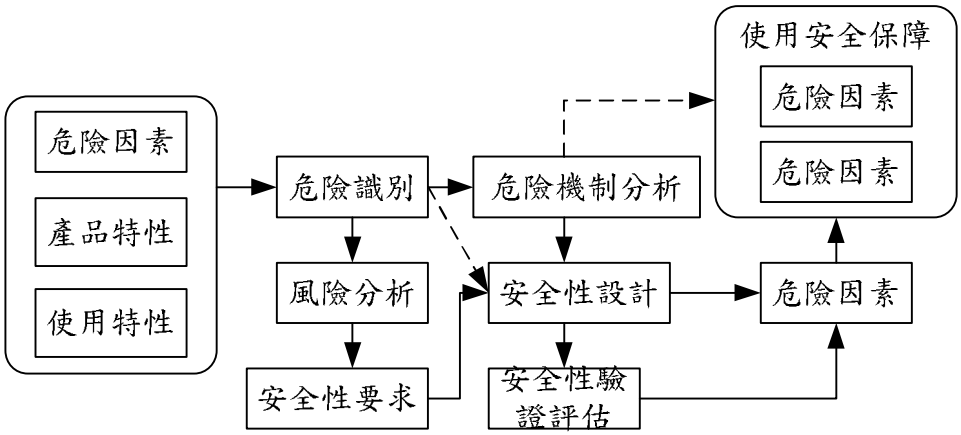


圖 3-1 安全性分析、設計和驗證工作之流程

安全性分析的主要目的在於識別危險，評估事故風險，以便在產品壽命周期的備個防階段中能夠消除或控制這些危險。提高產品的安全性，使其不發生或少發生事故，其前提條件是預先識別系統可能存在的危險，全面掌握其特點，明確其對安全性影響的程度。在系統壽命周期備個階段展開安全性分析的作用主要展現在以下幾個方面：

(一) 識別產品中所有可能存在的危險；

(二) 確定系統設計的不安全狀態以及與危險有關的系統流程；

(三) 分析危險引發事故的原因、過程和後果；

(四) 結合已採取的安全性措施，評估危險導致事故的可能性、嚴重性和事故風險；

(五) 依據預先確定的規則劃分危險類別，確定安全性關鍵項目和殘餘風險；

(六) 提出分析結論和評估意見，為後續安全性設計、驗證、評估和工程決策活動提供參考和依據；

(七) 分析結果可支持安全性驗征工作。

3.2.1 安全性分析的輸出結果

通過安全性分析，可以給出系統中存在的安全性問題，特別是重大安全性問題。安全性分析工作的輸出結果或結論主要包括以下內容：

(一) 後續工作安排，包括試驗、培訓、其他分析工作等；

(二) 可能導致事故或不安全操作的危險模式；

(三) 安全性相關的設計規則、規範或要求；

(四) 需要綜合考慮的安全性因素；

(五) 安全保護措施的評估結論以及實施這些措施的優先順序；

(六) 系統或子系統接口存在的安全性同題；

(七) 導致事故的備業因素；

(八) 危險事件可能性的量化評估結論及關鍵路徑；

(九) 事故風險排序及結論；

(十) 用於訂定緊應方案、設計防護設施設備、安排人員訓練計劃所需要的資訊；

(十一)與安全法律法規、規章制度的符合程度的結論意見。

3.2.2 安全性分析的基本流程

安全性分析是基於系統工程的原理和方法，識別、分析產品中存在的危險因素，並根據實際需要對其進行定性、定量描述的工作過程。通過個過程，可以充分了解、識別系統中存在的危險，估算事故發生的機率和可能產生傷害及損失的嚴重程度，為確定出哪種危險能夠通過修改系統設計或改變控制系統運作程序來進行預防提供依據。

為確保可滿足預期的安全性要求，在制定過程中應展開安全性分析工作。安全性分析應從設備研發階段早期開始並貫穿整個壽命週

期。在不同階段，由於可獲取的數據及資訊的不同，安全性分析的重要也有所不同。通常在驗證階段和方案階段初期，安全性分析重點在於考察設備的固有危險特性，即識別分析第一類危險源；在方案階段後期和工程研發階段，安全性分析的重點是第二類危險源，對故障、流程以及產品使用操作等有關的危險進行全面分析和綜合評估。即使備階段的分析工作不同，分析目的也備有差異，但每一類安全性分析的基本流程是一致的(圖 3-2)，主要包括以下工作：

(一) 定義系統邊界和組成部分，明確系統的要求和技術特性，包括任務階段、工作方式、使用環境以及人員安排等；

(二) 識別系統中所有潛在危險，分析造成危險的原因、可能的後果以及各種危險之同的關係；

(三) 對危險進行排序，按照預先規定的規則進行風險評估；

(四) 提出消除或控制危險的安全性措施；

(五) 提出安全性的驗證方法和時機；

(六) 結合提出的安全性措施，評估系統事故風險降低的程度，檢驗措施的有效性；

(七) 分析殘餘風險，通過決策確認風險是否達到可接受的程度

(八) 對系統中的危險和殘餘風險持續追蹤

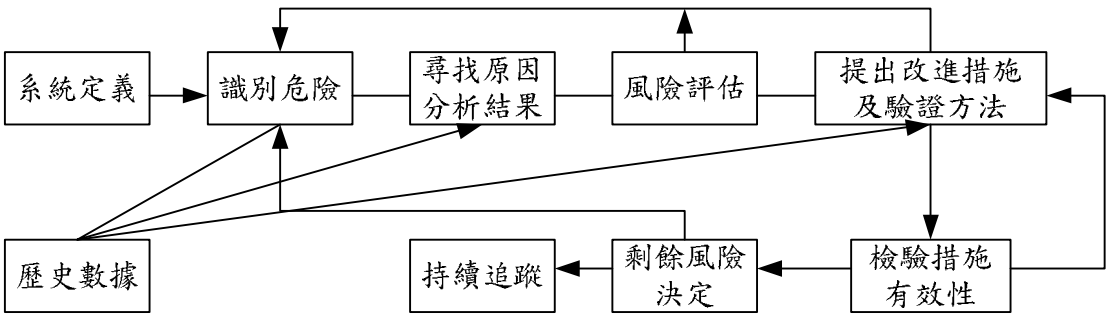


圖 3-2 安全性分析基本流程

3.3 安全性分析工作及方法

設備的安全性分析及風險評估工作是一個反覆替代、不斷改善的過程，應該在設備開發的早期就開始實施，而隨著開發工作的進展、可獲得的數據和資訊的增加，然後在不同的壽命周期展開不同類型的分析工作，以滿足設備安全性要求。

3.3.1 安全性分析工作流程

安全性分析工作包括工作項目和分析方法。在產品壽命週期的早期進行分析是最經濟有效的，因為在這時通過設計修正消除或控制危險是比較容易的。通常在驗證和方案階段進行分析的費用最低，在工程開發和生產階段的費用迅速增長，在使用階段費用最高。參照 GJB900-1990 的要求，產品在開發、生產近程中主要運用的安全性分析工作包括：在驗證階段編制初步危險表(PHL)和運用初步危險分析(PHA)、安全性要求分析(SRA)；方案階段運用子系統危險分析(SSHA)；工程開發階段運用系統危險分析(SHA)、使用和保障危險分析(O&SHA)以及職業健康危險分析(OHHA)。

產品壽命週期備階段安全性分析工作流程如圖 3 -3 所示。備階段的工作重點如下：

(一) 驗證階段。提出安全性要求和安全性工作要求，編制 PHL，宏觀確定危險的範圍。

(二) 方案階段。制定安全性大綱及工作計劃，運用 PHA，確定產品及其系統的安全性要求。擬定安全關鍵項目清單，依據安全性分析結果進行方案權衡；總體單位提出對安全性及其工作要求。

(三) 工程開發階段。深入運用安全性分析與設計工作，安全性評定、驗證與評估。結合操作規程對產品使用中的危險進行分析，制定使用安全規程和緊急方案。

(四) 生產階段。工程更改和技術狀態更改的安全性分析與驗證評估，收集並回饋資訊。

(五) 使用階段。收集、回饋使用安全性資訊與事故調查訊息，必要的設計更改與安全性驗證評估，以及安全規程與緊急備案的訓練、使用與修訂。

(六) 退役階段。危險物質暨材料的處置，防止人員傷亡和環境破壞。為完成各項分析工作，需要採用具體分析方法展開工作。通常會選取一種或幾種方法來完成一項分析工作。常見的定性分析方法包括功能危險分析(FHA)、故障模式及影響分析(FMEA)、故障樹分析(FTA)、潛在通路分析(SCA) ，事件樹分析(ETA)、意外事件分析(CCA)、區域安全性分析(ZSA)、接口分析(IFA)、電路邏輯分析(CLA)、環境因素分析(EFA)等。定量分析方法包括故障模式、影響及危害性分析(FMECA)、故障樹分析(FTA)、概率風險評估(PRA)等。

這些分析方法各有自己的特色，但也存在交叉相似之處，使用中應依據系統的特色、分析的要求和目的及分析時機，選用適當的分析方法。在分析過程中，必要時要根據實際需要對其進行修正和簡化，並且應從系統原理出發，開發新方法，形成新的系統性的安全分析方法。

3.3.2 常用的安全性分析方法

安全性分析方法包括定性分析和定量分析。定性分析用於檢查、分析和確定可能存在的危險、危險可能造成的事故、以及可能的影響和防護措施。常用的定性分析方法包括：故障危險分析、功能危險分析、故障模式影響分析、故障樹分析、潛在通路分析、事件樹分析、意外事件分析、區域安全性分析、接口分析、電路邏輯分析、環境因素分析等。除了上述分析方法外，在對具體系統進行備類危險分析時，根據需要還可採用表格危險分析法、標示法、立體模型法等作為輔助分析方法。

定量分析用於檢查、分析並確定具體危險、事故影響及其可能發生的概率，比較產品採用安全措施或更改設計方案後概率的變化。目前，定量分析主要用於比較和判斷不同方案的系統所達到的安全性水平，作為對有關安全性更改方案錯誤的基礎。定量分析必須以定性分析作為依據，常用的定量分析方法包括；故障模式影響及危害性分析、故障樹分析等。為了能準確估算產品可能發生事故的概率，比較有效的方法是概率風險評分方法。

目前對產品安全性進行定量分析往往存在較大困難，其問題不是分析方法本身，而是由於缺乏可用的安全性數據。當前可能獲得的有效的定量數據只是電子元器件的失效率數據，各種大的機械、機電設備的故障率數據很少，而且由於環境條件、維修工作等方生的影響，數據的可靠程度差；此外，有關人為出錯、環境因素和設備的危險特性的數據更少，更不可靠。因此定是分析方法在實際工程中的應用受到了侷限。

在具體的安全性分析中，可根據被分析對象的特點，選擇一種或幾種分析方法組合已滿足所規定的分析要求，在選擇方法時，應

考慮下列兩條準則：(1)分析應當盡量廣泛，確保可能有效地辨別和評估所有的危險；(2)對每種危險的分析應盡可能徹底和準確。

3.4 表格危險分析法

危險分析法的種類有很多，在這個研究中我們先介紹表格危險分析法，該方法用來檢查軟硬體系統在各種使用模式中或使用模式本身存在的危險，分析人員通過該方法全面、系統地識別潛在的危險源和危險狀態，分析發生危險的原因和危險後果及影響，預計這些危險對人員傷害或對設備破壞的嚴重性和可能性，進行定性風險評估，並提出相應的控制措施或緊急方案來消除或減少危險，以便在發生事故之前消除或盡量減少事故發生的可能性或降低事故有害影響的程度。表格危險分析法屬於定性分析方法，由具有技術人員、操作人員和安全管理人員實施。利用對方法進行分析或總結歸納已有安全資訊及其相關風險控制措施可以保證分析結果層次分明，條目分明，易於理解，在實際工程中應用最為廣泛。

利用表格危險分析法進行危險分析通常可達到以下目的；

(一) 盡早識別出系統存在的危險源以及相應的危險狀態，確定安全性關鍵因素；

(二) 分析危險發生的原因以及後果影響；

(三) 確定危險的嚴重性和發生的可能性，進行定性的風險評估；

(四) 確定安全使用準則，提出消除或控制危險的措施，解決系統中存在的安全問題。

3.4.1 分析過程及步驟

危險分析法的核心在於利用表格形式所具有的層次鮮明、條理清晰、簡要直觀等特點，對系統備層次及分析範圍的危險進行識別，並分析危險的原因、潛在的事故影響等。在安全性工程分析工作中，利用表格進行分析是備個工程階段、各種分析類型的總體形式。在不同的工程階段，表格危險分析法的應用方式和著重內容有所不同，隨著系統開發工作的進展，表格危險分析法以不同的危險分析形式出現，如初步危險表(PHL)、初步危險分析(PHA)、子系統危險分析（SSHA)、系統危險分析(SHA)、使用和保障危險分析(O & SHA)，以及職業健康危險分析(OHHA)等，但這些不同類型的危險分析從方法本身而言仍體現出明顯的共同特性。

表格危險分析法基本框架如圖 3 -4 所示。其中內容根據分析類型及所在開發段的不同需進行修正和確認。

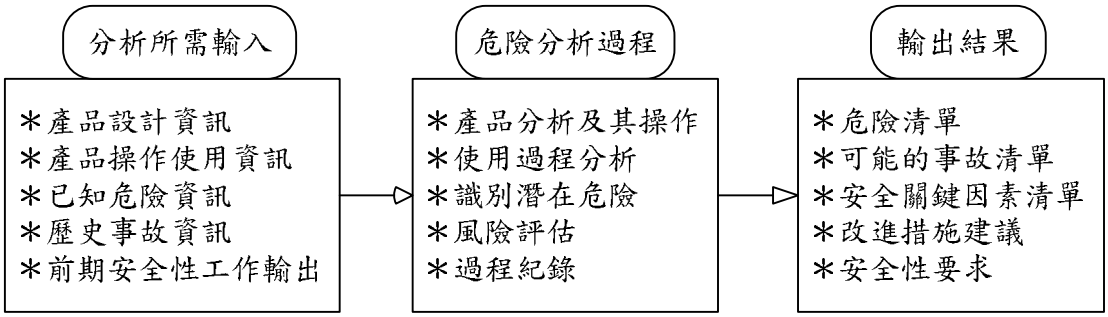


圖 3-3 表格危險分析法基本架構

表格危險分析法要求分析人員應從工作說明、設計規範、設計圖紙等資料中獲取對所分析對象的設計要求、使用條件和要求、組成結構和軟硬體功能原理等設計資訊，最好還能掌握功能框圖、可靠性框圖、操作使用要求等資訊。同時應對危險、危險來源、危險

的構成要素、以及相似產品對象所發生過的危險及安全事故具有較深人的了解。

3.4.2 分析形式

表格危險分析法利用表格記錄分析過程及其中所產生的資訊，為所識別的危險的可信性提供足夠的支持依據，只有知道工程規定的表格形式、表格填寫規則和利用表格的分析思路才能充分有效地運用安全性分析工作；只有統一表格內容定文、表格分析層次以及表格分析的用語和符哥，才能協調工程中備部分安全性分析工作，做到不遺漏系統危險。表格的主要作用在於為分析過程提供思路框架以及便記錄訊息，表格形式本身是可變的，這裏僅列舉典型的表格形式以便說明，如表 3 -2 所列。對於表中備項內容的填寫說明詳見下節。需要說明的是，不同類型的危險分析所採用的表格形式有一定差異，依根據分析要求及分析時機對該表格形式進行適當地調整。

表 3-1 表格危險分析法典型格式

XX 類型危險分析								
分析對象(層次)(1)						分析人員及日期(2)		
序號	分析項目	危險原因	危險	所處階段	危險影響	風險評估	建議措施	採取改進措施後的風險
(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)

為了加強安全性分析和評估結果對系統設計的指導作用，落實改進措施，在完成填表分析之後，還應對分析結果進行歸納總結，主要包括以下內容：(1)將識別得到的危險按照其風險水平由高到低進行排序，並列出清單；(2)對分析得到的安全關鍵因素列出清單，並盡可能明確設計改進措施所對應的系統組成部分。

3.4.3 表格填寫說明

本節對表 3-1 中各欄內容如何填寫給出詳細說明，對應欄位依次簡述如下：

(1) 分析對象：該欄應填入所已確定的分析對象，例如系統硬體、功能、軟體、能量源等。也可以是某項操作或使用任務。

(2) 分析人員及分析日期。

(3) 已識別的危險的序號。

(4) 分析項目。該欄位應填入欄位(1)中所填分析對象的主要組成部分。分析對象首次被分解為系統硬體、功能、軟體、能量源等，應通過詳細檢查假定被分解出的四個項目中可能存在的危險，例如，爆炸物可列在以“系統硬體”為分析層次的表中，也可列在以“能量源”為分析層次的表中。如果欄位(l)中所填內容為某項操作或使用任務，此處則對應填寫組成任務的事件活動或步驟，並盡可能包含操作使用任務的目標、模式或所在階段訊息。為了確保能夠識別出與爆炸物相關的全部危險，允許在一組分析表中的內容有一定重疊。

(5) 本欄確定可能導致危險的條件、事件或失誤，以及可能觸發危險物質引起事故的觸發事件。針對攔位(4)所列出的項目進行逐項分析，針對每一項考慮可能觸發危險的各種情況；

(6) 本欄填寫已識別出的分析項目所具有的危險。本欄所填寫的危險和攔位(5)所填寫的發生該危險的原因立明確對應，可採取以下方式對危險進行識別：

(a) 結合歷史事故數據、相似產品危險數據識別系統的相關危險；

(b) 根據工程經驗識別出可能發生的危險，包括系統故障對系統的危害，對人員的傷害和對環境的破壞等；

(c) 合理運用專業知識、相關訊資和分析產品的功能原理，結合危險源演變為事故的原理過程，識別產品潛在危險；

(d) 組織備專業人員以開會的形式進行對論可能發生的危險，務必記錄所有潛在的危險，即便後續分析證明該危險是否存在。

(7) 該欄確定所識別危險發生時，系統可能所處的運作模式、任務階段以及使用場景、或系統遭遇的可能導致危險的條件，從而輔助進行安全性設計和給出安全性要求。

(8) 該欄用於識別危險的影響和後果。針對前面所識別出的每一個危險，由危險造成的各種有害影響。有害影響主要包括某一危險導致的系統喪失、損傷；造成對人的傷害，甚至死亡；或是造成嚴重的環境破壞。在進行危險影響分析時，需要注意以下問題：

(a) 在填寫危險影響一欄時，該影響是假設未採取相關安全措施的情況下，危險可能造成的傷害程度最大的影響；

(b) 分析在不同的系統狀態或工作階段時，危險發生後可能發生局部影響、高一系統層次影響和對系統的最終影響。在分析危險對系統的影響時，該欄填寫的內容主要是某一危險對整個系統的最終影響。

(9) 風險評估。在未採用相關技術進行危險減少的前提下，定性地評估已識別危險的潛在事故風險，風險評估是事故嚴重性和事故發生可能性的綜合表現。事故嚴重性和事故發生可能性等級判定準則可參閱前章 2.2 節。

(10)建議措施。該欄填寫用於消除或減輕已識別危險的預防性措施建議，並盡可能明確在什麼情況下採取什麼形式的措施(控制措施和補償措施)。通常以安全性要求準則的形式給出，並應轉化為系統安全性要求。

控制措施一般分為兩類：

(a) 設計補償措施。設計補償措施是用來從設計上消除風險，或將風險減小到可接受範圍的一種安全性工程手段。設計補償措施是控制風險的首要工作，在建議設計補償措施時，設計者還應考慮技術條件、項目進度、系統周期費用等限制。設計補償措施通常包括選取設計方案、改進設計等。

(b) 使用補償措施。使用補償措施是使用階段採取的安全控制措施。使用補償措施目的是為了減少設計流程中沒有消除的風險。使用補償措施的手段為了盡量避免或預防危險發生，在正常使用和日常維修中規定一些使用的維修措施和操作流程，一旦危險發生，操作人員立刻根據現有的緊急備案採取最恰當的補救措施，將危險的影響程度降至最低。使用補償措施通常包括：安全保障裝置、警告裝置、確定安全操作規範及人員培訓等。補償措施的制定和採納應遵循以下優先順序：(i)通過選取設計方案消除危險;(ii)通過改進設計控制危險；(iii)通過安全保障裝置控制危險；(iv)通過告警裝置控制危險；(v)通過確定安全操作規範及人員培訓控制危險。

需要思考的是，應盡可能考慮所建議的改進措施可能引入的新的危險，以及對風險評估結果帶來的變化。

3.5 能量跟蹤與屏蔽分析

3.5.1 ETBA 理論

產品的運作需要各種必要的能量，而武器產品而言為了消除或摧毀敵方有效力量和設備、設施更需要能量，因此產品總會存在類必要能源而無法在設計方案中徹底消除。產品中的能源既是武器殺傷力的基礎，也是潛在的危險因素，需要在設計、使用過程中對其認真分析，避免引發事故。能量跟蹤與屏蔽分析(Energy Trace and Barrier Analysis , ETBA)的目的就是要評估這些危險源，判斷設計方案中與其相關的潛在危險是否已通過能量屏蔽得以消除或將風險降低到可以接受的程度。

ETBA 是一種用於識別分析與有害能源相關危險的技術方法。通過對危險能量源屏蔽措施的評估，ETBA 提供了可讓不希望或異常能量源對人員或設備危害的方法。它是一種識別能源相關危險的有效安全性分析方法，與其他分析方法相比，結構化的 ETBA 方法能夠避免主觀影響，得到前後一致、理由充分、符合邏輯的結論。ETBA 也可被簡稱為能量跟蹤分析或屏蔽分析。

ETBA 技術通過識別可能會引起危險的能量源路徑，分析且制訂必要的屏蔽方案以避免能量源造成設備損壞或人員傷亡。通過依次對系統中的能量源(包括輸人和輸出能量源)詳細規範的跟蹤分析，ETBA 能夠對每一類能量進行徹底的分析。在產品設計過程中可以採用不同類型的能量屏蔽方式，如物理屏蔽(防護罩)、程序屏蔽等。事實上，屏蔽可以理解為針對特定能源類型的任何可以降低事故可能性或後果嚴重性的措施。

ETBA 能夠對在研發或現有產品進行詳細分析，可用於支持 PHA、SSHA 和 SHA 分析工作，對 O&SHA 分析工作和事故調查也能有所幫助。

為了做好 ETBA，需要對產品中的各種類型的能源及其行為有一個全面詳細的認識，還需要認真分析產品的設計和運作方案。因此在不同的階段，應根據掌握的產品資訊來提昇 ETBA 分析。但是，ETBA 的分析範圍存在局限性，其重心是產品中的不同類型的能源和異常能量源，而不考慮造成危險的其他重要因素，如關鍵的人力失誤或設備故障，因此，它不是一個全面的安全性分析方法，無法單獨支持產品壽命周期備階段安全性分析工作項目的完成，需要與其他分析方法配合才能滿足全部分析工作要求。

3.5.2 ETBA 基本原理

最早由吉布森(Gibson)和哈登(Haddon)等人提出了解釋事故發生物理本質的能量意外釋放理論，認為事故是一種不正常的或不希望的能量釋放開並轉移於人體或作用於設備設施的過程或後果。它是 ETBA 方法的理論基礎。產品在運作中必須需要利用各種能量，必須對這些能量採取控制措施，使其按照人們的意圖產生、轉換和做功。從能量在產品中流動的角度，應該控制能量按照人們規定的能量流通渠道流動。如果由於某種原因失去了對能量的控制，就會發生能量違背人的意願的意外釋放或逸出，就可能會影響產品運行甚至發生事故。如果意外釋放的能量作用於人體，並且能量的作用超過人體的承受能力，則將造成人員傷亡；如果意外釋放的能量作用於設備、建築物等，並且能量的作用超過它們的抵抗能力，則將造成相關的損壞。現代產品中存在各種形式的能量，如機械能、熱

能、電能、化學能、輻射能等，它們的意外釋放都可能造成傷害或損壞。表 3-2 和表 3-3 列出了一些常見能量類型能造成的人員傷害和事故類型。

表 3-2 能量類型與人員傷害

能量類型	產生的傷害	事故類型
機械能	刺傷、割傷、撕裂、骨折	車輛傷害、機械傷害、墜落、壓力、容器爆炸
熱能	皮膚發炎、燒傷	燒燙、火災
電能	干擾肌肉神經、電傷	觸電
化學能	皮膚炎、燒傷、癌症	中毒、窒息、火災
電離輻射	細胞成分破壞	放射性粉塵、同位素

表 3-3 干擾能量類型與傷害

影響能量交換類型	產生的傷害	事故類型
氧的利用	局部或全身生理損害	中毒和窒息
其他	局部或全身生理損害、熱經攣、熱衰竭	

能量意外釋放理論闡明了事故發生的物理本質，指明了防止事故就是防止能量意外釋放，防止人體或設備接觸異常能量。從該理論出發，預防事故就是要防止產品中的能量或危險物質的意外釋放，防止人體或設備與過量的能量或危險物質接觸。把約束、限制能量，防止人體或設備與能量接觸的措施叫做屏蔽。這是一種廣義的屏蔽，並且不侷限於具體的屏蔽設備，還包括從時時、空間或程序上的屏蔽。

在 ETBA 中，事故危險是指系統中能量的異常流動，當缺乏足夠屏蔽而使異常能量源沿某一路徑運用，導致人員傷亡或設備損壞，就引發了系統發生事故。ETBA 認為任何事故都是由三類因素組

成的(圖 3 -4)包括異常能量源，能量路徑所經過的人員和設備設施以及能量與目標之間的屏蔽。當屏蔽不足以阻止或控制能量源時，就會導致事故的發生。因此 ETBA 就是要系統地分析這三類因素及其相互關係，從而發現薄弱環節，通過改進設計以提高系統的安全性。

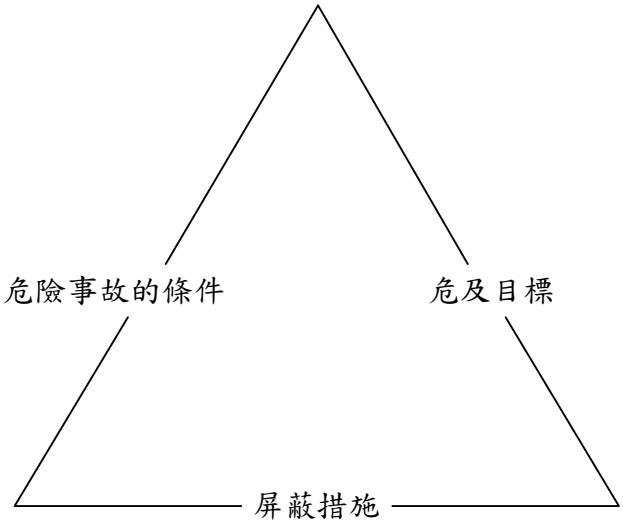


圖 3-4 基於能量釋放理論的危險構成因素

運用 ETBA 所需的基本資料是能夠顯示產品內部佈局的設計圖，其詳細程度應能滿足所需運用的分析工作要求。對於 PHA 來說，一個初步的草圖基本能夠滿足分析要求，要運用子系統危險分析或系統危險分析，則需要更加詳細的設計資料，除此之外，FTA 結果、維修保障和運行程序、設施佈局等資料都有助於分析的運用。

在研究產品安全性的問題時，基於任何事故影響的大小直接與所含能量有直接關係的原理，提出了通過控制能量來確保安全的方案。此外，事故造成人員傷亡和設備損壞的嚴重程度隨著失控的能量的轉移或轉換的大小而變化。因此，在產品的安全性設計中，能量是一個很重要的考慮因素。

安全性設計和分析人員必須了解上述這類事實，對具體的產品進行分析，確定可能發生最大能量失控釋放的地方，考慮防止能量轎轉移或轉換過程失控方法，及盡量減少不利影響的方法。這是設計一個安全產品必須做出的最大努力。

3.5.3 分析內容與實施流程

ETBA 基於能量釋放理論。產品中存在危險的能源時，它會對特定的目標造成威脅形成潛在的危險，在能源與受到威脅的目標之間設置屏蔽就可以消除這種危險或降低其風險。如圖 3-5 所示，它給出了一些常見的屏蔽方案。ETBA 需要認真地跟蹤分析產品中各種能量源。ETBA 認為事故的發生是由於穿過屏蔽的能量對目標造成的異常能量交換。ETBA 首先對產品設計方案進行分析，識別各種類型的能源，然後採用圖形的方式跟蹤從源頭到目標的能量傳遞路徑，並在恰當的位置標識出防止傷害的屏蔽。如果設計方案中沒有包含必要的措施，則設計人員應根據實際情況制定合理的屏蔽方案。

為了更好理解和應用 ETBA 方法，需要對幾個相關的概念做進一步的說明。下面是 ETBA 所相關的幾個基本術語：

(一) 能源(Energy Source)：任何包含了可以被釋放的潛在能量的材料、機械裝置或過程。關注的焦點是可能會傷害潛在目標的逸出能量；

(二) 能量路徑(Energy Path)：能量從源頭到目標所經歷的路徑；

(三) 能量屏蔽(Energy Barrier) ：任何阻止危險的能量達到潛在目標或將其強度降低到不會產生破壞或傷害程度的設計或管理措施。屏蔽採用各種方式將能源與目標隔離開來，

也可以採用不同的形式，如物理屏蔽、距離屏蔽、定時屏蔽、程序屏蔽等。

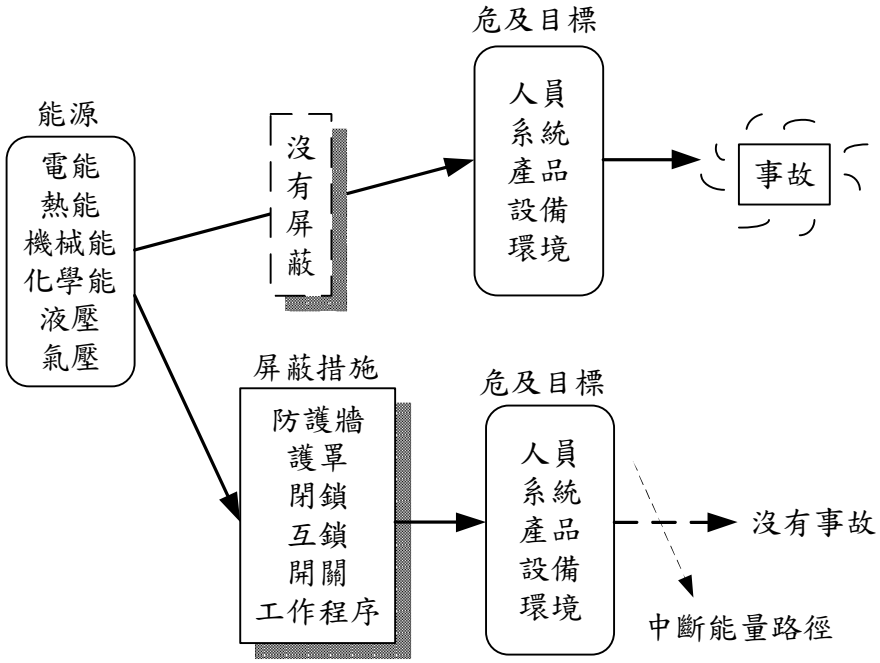


圖 3-5 能量屏蔽的作用示意圖

運用 ETBA，首先是識別產品中存在的各種類型的能量，然後確定每種類型的能量在產品中的位置，並跟蹤能量源或能量路徑以識別各種必需的屏蔽設備或方法。對備類屏蔽的保護效果進行評估，包括其對能量的控制和一旦失效可能危及的潛在危險目標。利用風險指數法對每一種異常能量源的風險進行評估，對不能接受的風險提出改進建議以提高產品的安全性水準。必要時可更改系統或子系統設計方案以消除危險，避免事故發生。ETBA 的基本流程如圖 3-6 所示。

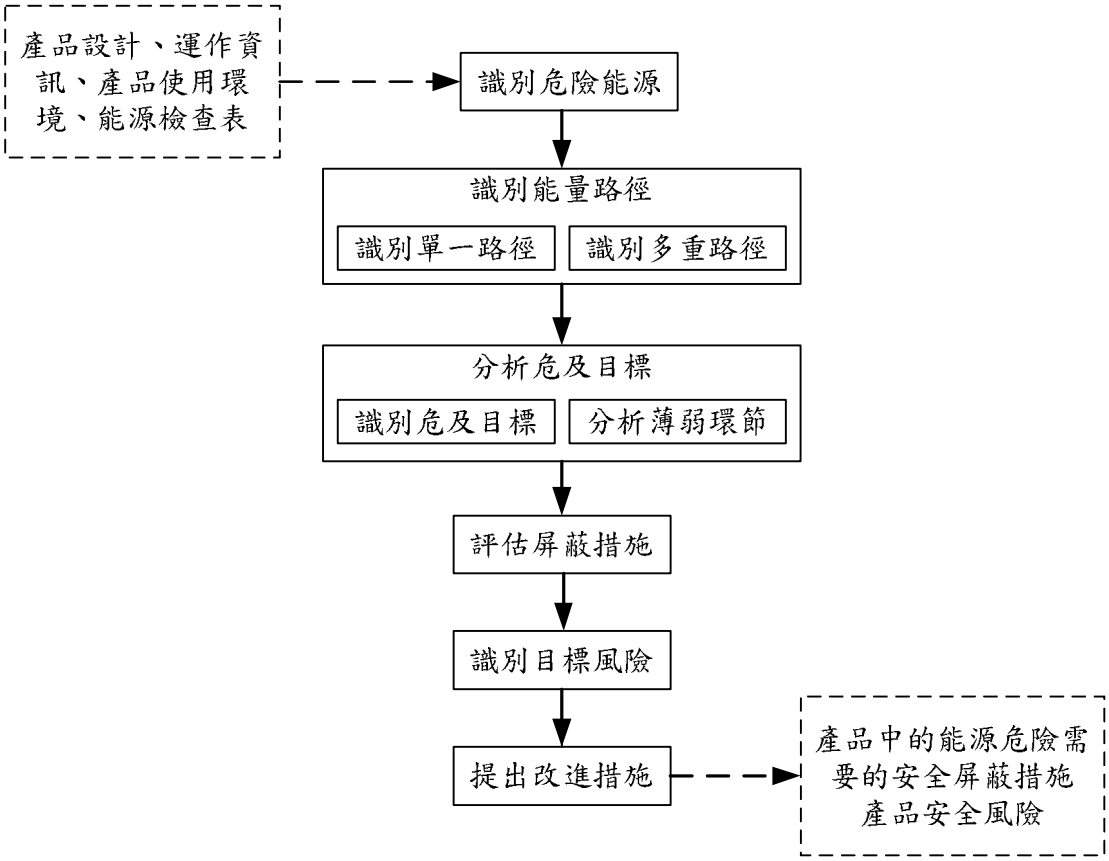


圖 3-6 ETBA 基本流程

(一) 識別能源類型。檢查產品或其設計方案，識別所有潛在的危險能源，如果有可能，還應掌握能源的數量、強度和位置。可以採用檢查表查找產品中的能量源，如炸藥、電磁輻射、電流、有毒物物質等。

(二) 識別能量路徑。從產品中的能源出發，識別 任何能夠導致事故的潛在的能量傳播或轉換的路徑。在很多情況下，同一種能源往往存在多重路徑到達同一目標或不同目標，應認真分析產品構成，確保全面課識別所有可能的路徑。可以採用圖形化的方式描述能量路徑，進而可以直觀地顯示能源、危及目標和屏蔽之間的關係。

(三) 識別危及目標。對每一種能源，從源頭開始跟蹤其在產品中的傳播或轉換路徑，識別各種可能會受到能量傷害或損壞的目標，包括人員、設備、設施、壞境等。採用圖示的方式能夠比較直現便捷地發現各種危及目標。

(四) 分析目標的薄弱環節。對於識別出的危及目標，應分析其對於特定能量的薄弱環節，以便進行風險評估或提出屏蔽措施建議。不同的對象對於同一種能量的反應是不同的，應結合產品的實際情況進行分析。例如，28V 直流電對人體基本上沒有任何傷害，但它卻能夠燒毀產品中的芯片，造成設備損壞。

(五) 評估安全屏蔽措施。跟蹤能量路徑，識別其中現存的各種安全屏蔽措施，或者分析路徑中應該設置的屏蔽；評估現存屏蔽裝置的保護效果，預測屏蔽失效或沒有屏蔽情況下的後果。分析時應與產品的任務階段相結合。

(六) 評估風險。對產品能源對危及目標可能帶來的事故風險進行評估，可以分別對存在和不存在屏蔽措施的設計方案進行評估，以便比對比各自的效果。

(七) 為提出改進措施。判斷現有屏蔽措施是否能夠滿足產品的安全性要求，如不能滿足，應對屏蔽措施提出改進建議以便消除危險或降低事故風險。必要時，應進一步進行更為詳細的分析(如故障樹分析)工作，確保所有危險因素都能夠被識別和控制消除。

(八) 提出分析報告。將識別出的危險回饋至 FRACAS 以便跟蹤後續工作，填寫能量跟蹤與屏蔽分析表，完成分析報告；必要時，應及時更新分析報告。能量能否造成傷亡或損壞取決於：接觸

能量的大小；接觸時間和頻率；能量的集中程度；屏蔽設置的早晚，設置的越早，效果越好。為屏蔽異常能量，可以從控制能源和減弱危害效果兩方面採取措施，通常採用的處理原則如下：

(1) 限制能量，如控制速度、溫度、壓力、電壓等；

(2) 用較安全的能源代替危險性大的能源；

(3) 防止能量蓄積；

(4) 控制能量釋放；

(5) 延緩能量釋放；

(6) 開闢釋放能量的渠道，如接地系統等；

(7) 設置屏障，如消音器、電磁屏蔽等；

(8) 在人員、設備與能源之間設屏障，如防護罩，防火門;

(9) 在人員與設備之間設置屏障，如防毒面具、安全帽、手套等；

(10) 提高防護標準，如採用雙重絕緣工具，連續監控，遠距遙控等；

(11) 改善效果及防止損失擴大，如緊急救援措施等；

(12) 修護或恢復。

根據能量的性質和強度大小，可以研究建立單一屏蔽或多重屏蔽措施。一定量的能量集中於一點要比它分散開所造成的傷害程度更大，因此，可以通過延長能量釋放時同或使能量在大面積內消散的方法來降低其危害的程度；對於需要保護的人和物應遠離釋放能量的位置，以此來控制由於能量轉移而造成的事故。需要注意的是，來自單一源頭的異常能源可能會危及多個目標，而為了提高產品的安全性水準，很可能需要多重屏蔽。

ETBA 詳細分析了產品中的能源以及它們對人員或設備的潛在影響，最終的分析結果可以採用表格的形式。針對不同的產品特點和分析要求，可以採用不同形式和內容的 ETBA 分析表格，但通常應該包括以下內容：

(一) 產品中會造成威脅的能源；

(二) 可能會受到能量傷害的目標；

(三) 現有的能夠控制能量危險的屏蔽措施；

(四) 建議的用於控制能量危險的屏蔽措施

(五) 與能量-屏蔽危險相關的系統風險。

常用的 ETBA 表格，如表 3-4 所列。

表 3-4 ETBA 典型格式

能源	能源危險	危及目標	初始風險指數	屏蔽措施	最終風險指數	備註
(1)	(2)	(3)	(4)	(5)	(6)	(7)

分析表中各列的含義如下；

(1) 能源。產品中識別出的各種危險能源。

(2) 能量危險。描述與識別出的能源相關的危險，包括能量路徑的說明。應盡量說明危險的效果和可能的事故後果以及各種相關因素，包括可能軟硬體故障、人力疏失等。

(3) 危及目標。當沒有屏蔽或屏蔽失效時能量可能危及的目標。

(4) 初始風險指數。對識別出的危險導致的事故風險判定測量，該指數應該反映的是沒有屏蔽措施時的風險。可採用第二章中的風險劃分等級，也可根據實際情況確定。

(5) 屏蔽措施。在採取屏蔽措施時，應遵循如下優先次序：

(a) 通過設計手段消除危險或降低其風險；

(b) 利用安全裝置降低事故風險；

(c) 利用警報警裝置降低事故風險；

(d) 利用安全規範和培訓降低事故風險。

(6) 最終風險指數。採用了屏蔽措施後的風險指數。應採用與初始風險指數相同的風險劃分等級。

第四章 事故產品安全性調查-開飲機

4.1 前言

承前兩章所說明的安全性量測、要求及其分析，可將其理論架構實際上的運用在事故風險較高的開飲機之產品上，期望透過這些理論的有效運作，能夠找出導致危害的原因，進而可提出修正的建議可用以回饋於安全性設計上的考量。如此一來，安全性設計即可透過修正之設計理念來消除和控制各種危險，提高產品的安全性。

4.2 開飲機產品事故類型

以目前本局所得事故通報之資訊，開飲機產品事故類型皆著眼在於燃燒，其該模式如果早期發現僅有財物損失；假使發現得晚，有可能造成更嚴重的人員傷亡及環境毀壞。

那麼，為何會引發燃燒?這時候我們首先要先了解著火理論，燃燒即是著火所引起。

4.2.1 著火理論

燃燒過程一般可分為兩個階段，第一階段稱為著火階段，第二階段即為著火後的燃燒階段。在第一階段中，燃料及氧化技進行緩慢的氧化作用，氧化反應所釋放的熱量只是提高可燃混合物的溫度及累積活化分子，並沒有形成火焰。在第二階段中，反應進行的很快，並發出強烈的光與熱，形成火焰。

4.2.2 熱著火反應

熱著火是在利用外部能源加熱(如電火花、電熱絲、熱的接觸和

壓縮等)的條件下，使反應混合物(可燃劑及氧化劑)達到一定的溫度，在該溫度下反應混合物化學反應所釋放出的熱量大於它向周圍環境的散熱，從而使反應混合物的溫度進一步升高，接著溫度的升高又進一步導致化學反應速率和放熱速率的加快，如此陸續地循環，最終造成全面的燃燒反應。

對於一個放熱反應，如果在嚴酷的高溫條件下，只要反應物的量足夠，則都可能發展為著火，也就是所謂的自燃。也就是說只有當反應物消耗殆盡才能使得這種自加熱反應不會發展到著火的程度。另外一種情況，雖然沒有外部的熱源，也沒有嚴酷的高溫條件，這在種狀態下只要本身的熱分解(或氧化或混合物的相互反應等)所放出的熱量大於該情況下它向外界的散熱，此時只要反應物的，也會發展成著火甚至爆炸。

4.2.3 表格危險分析法-開機機

在本研究中，以隨機抽樣的方式由某品牌開飲機(已使用三年)當成測試樣品進行分析，首先進行表格危險分析法及 ETBA 分析前需要知道該事故產品之能源、能量路徑以及能量屏蔽。其中，能量路徑以及能量屏蔽即為一體兩面的事物；以燃燒這個作用而言，能量路徑即是要找出能可燒及延燒的物質或組件；而能量屏蔽即是反向的考量，能夠有效的去阻止燃燒，本身不會燃燒，然而亦不會由其他熱源來引燃。

表 4-1 開飲機事故產品危險分析表格

開飲機事故產品危險分析								
分析對象(層次)(1)						分析人員及日期(2)		
序號	分析項目	危險原因	危險	所處階段	危險影響	風險評估	建議措施	採取改進措施後的風險

(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)

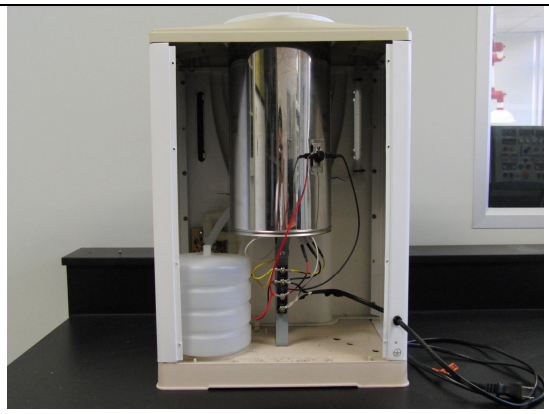
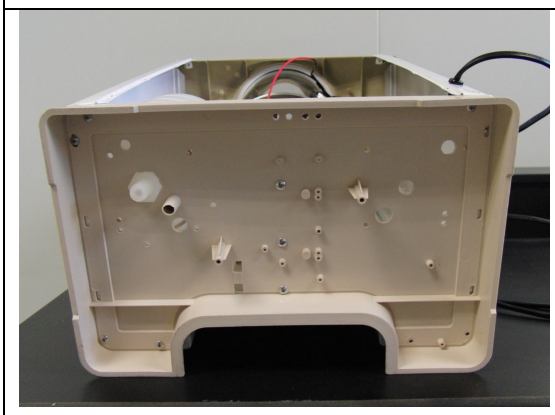
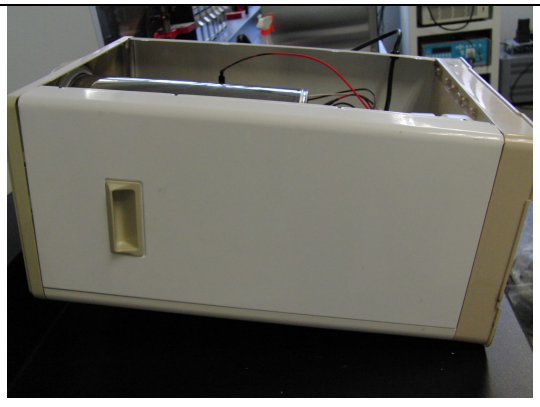
表 4-2 開飲機事故產品 ETBA 分析表格

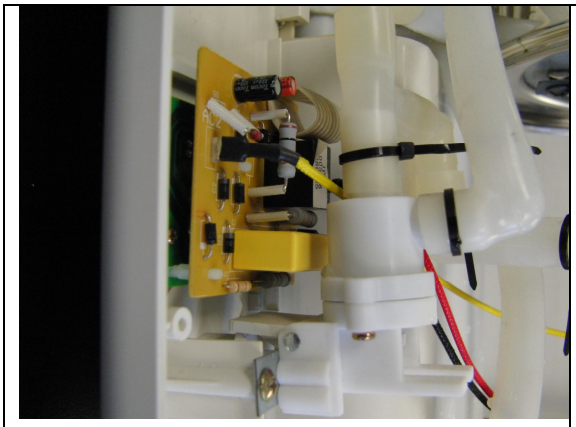
能源	能源危險	危及目標	初始風險指數	屏蔽措施	最終風險指數	備註
(1)	(2)	(3)	(4)	(5)	(6)	(7)

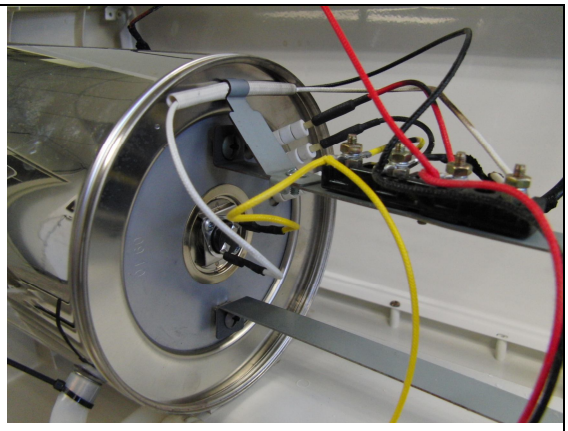
4.2.4 開飲機分解圖

由下面多圖可看出，開飲機是由前後外殼、左右側殼、上蓋、底座、塑膠溫膽、不銹鋼熱膽、矽膠軟管、塑膠硬管、電子元件、PCB板、水源開關、生水阻隔開關、內部配線、電源線、O-RING、電子元件、端子座及鐵支架所構成。

表 4-3 開飲機外觀圖





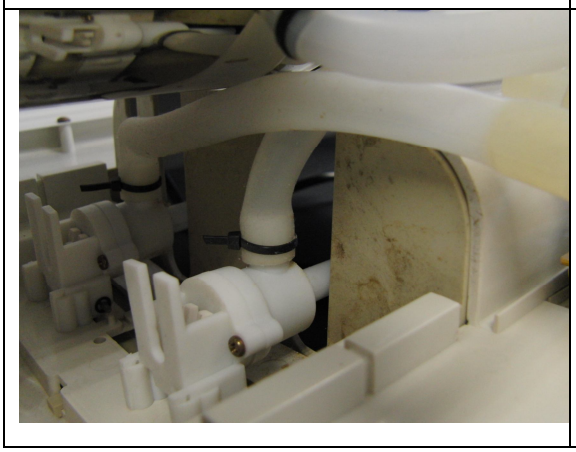
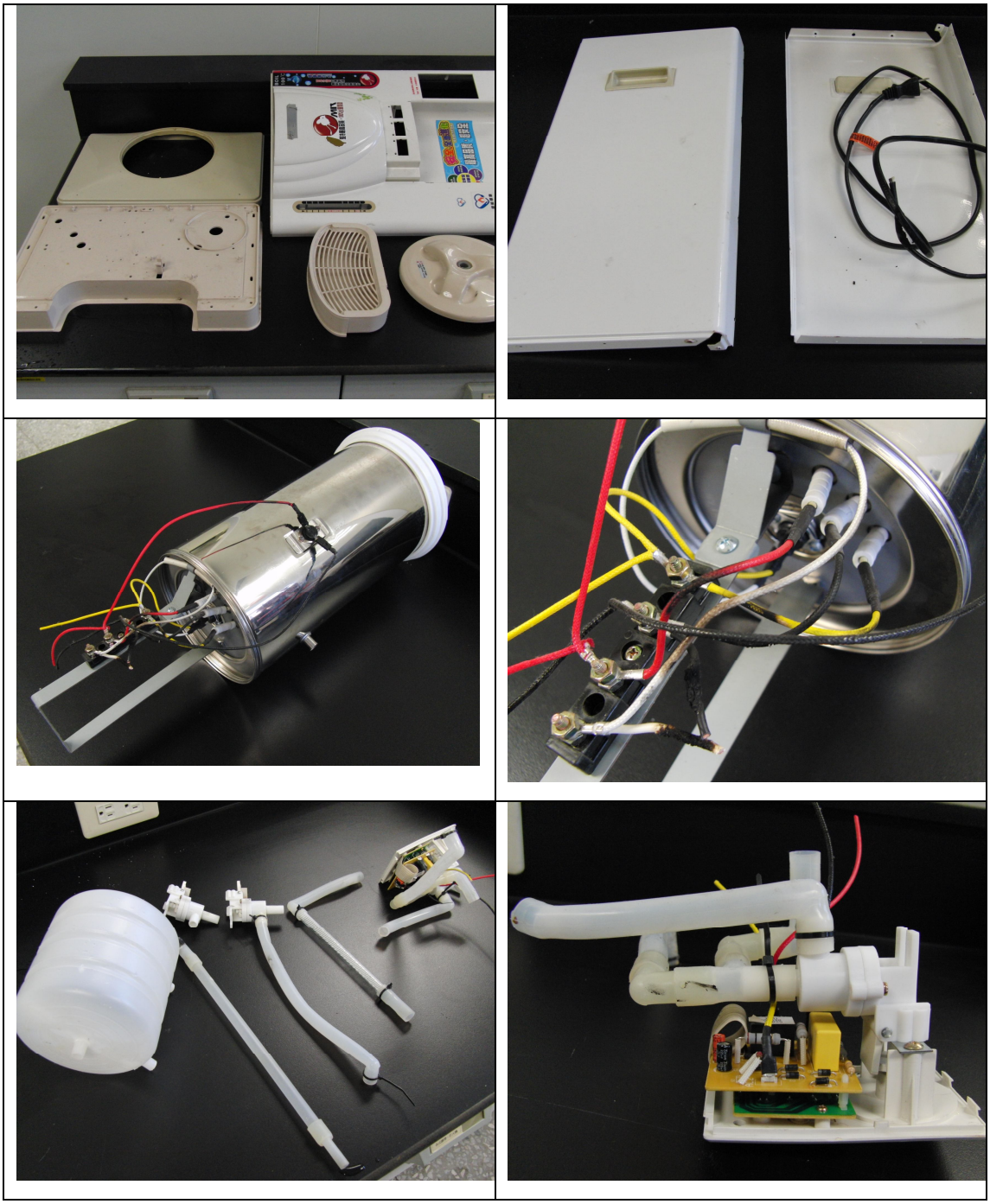


表 4-4 開飲機拆解圖



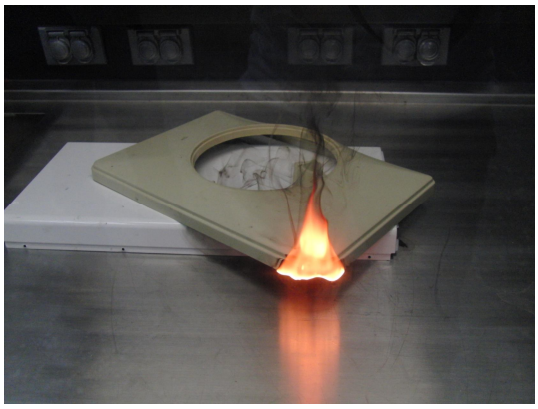
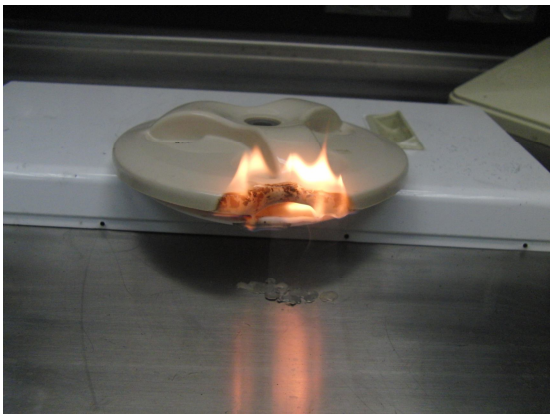
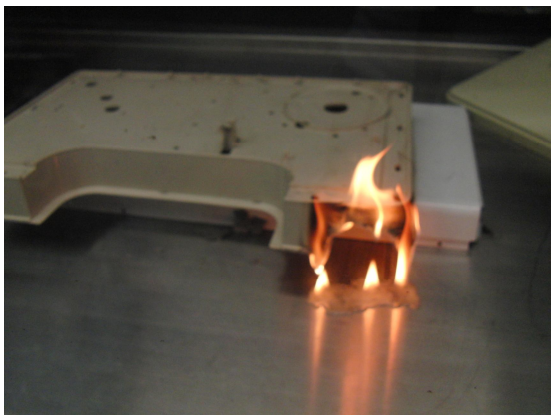
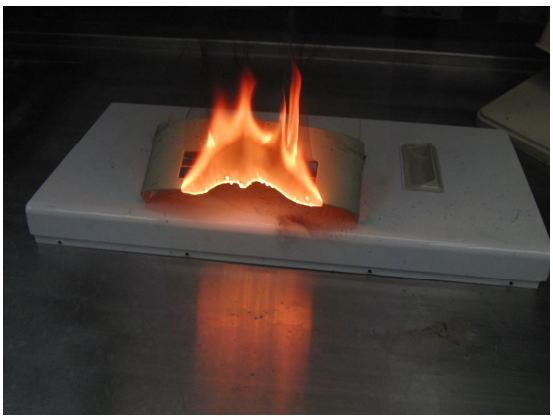
由分解出的各部位、儼然如一概略爆炸圖。再之，即可以材質分類將其劃分為兩大類；其中一類為金屬類，另外一則歸為非金屬類。其中金屬類包含左右側殼、不銹鋼熱膽及鐵支架；而前後外殼、上蓋、底座、塑膠溫膽、矽膠軟管、塑膠硬管、電子元件、PCB 板、

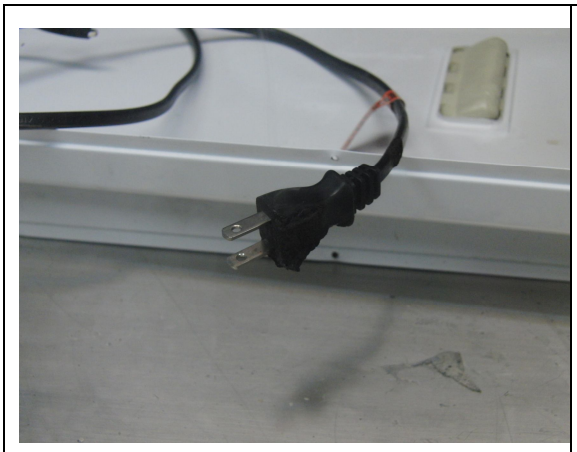
水源開關、生水阻隔開關、內部配線、電源線、O-RING、電子元件則是納入非金屬類的一員。如此一來，我們僅要對後者進行考量即可。因為金屬的材質既不會自燃亦不會延燃，因此可直接將其定義為安全之部件。金屬的材質以外的部件將由下節進行試驗。

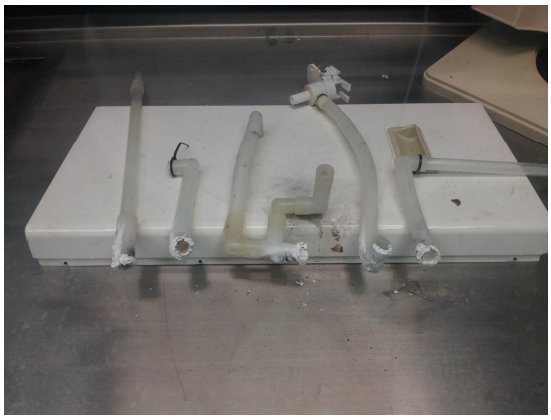
4.3 開飲機非帶電部位進行燃燒試驗

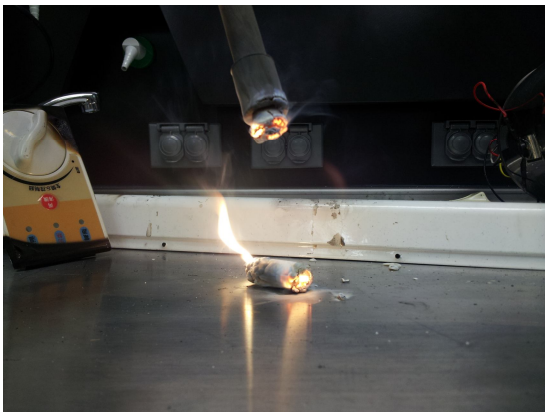
針對非金屬類中的前後外殼、上蓋、底座、塑膠溫膽、矽膠軟管、塑膠硬管、水源開關、生水阻隔開關及 O-RING，進行燃燒試驗

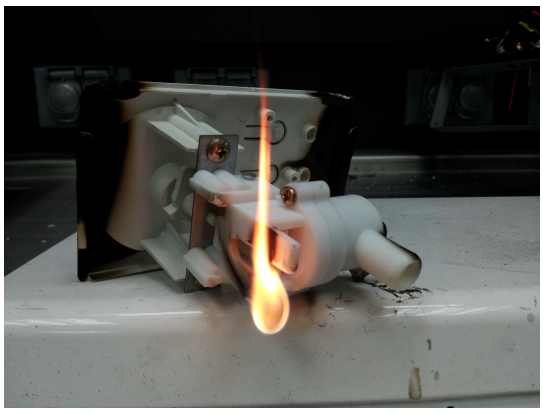
表 4-5 開飲機非帶電部位燃燒試驗圖

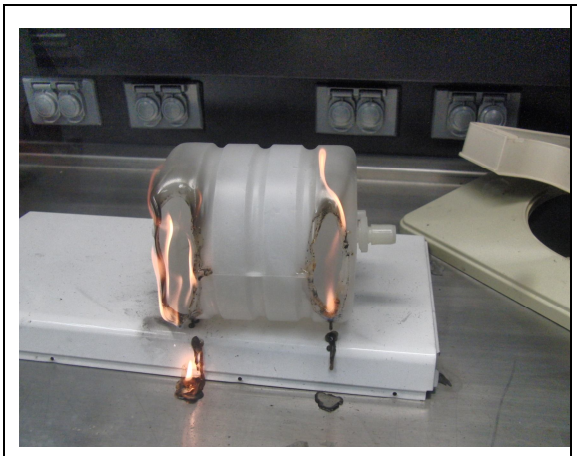
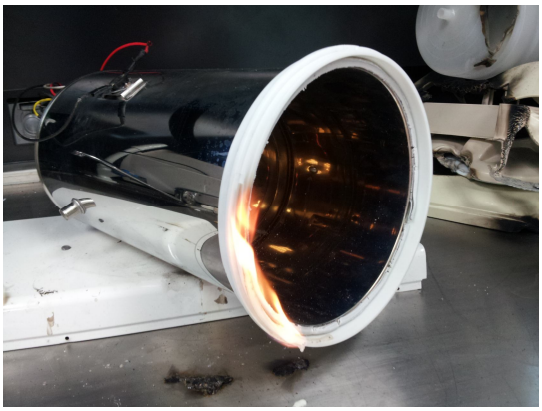











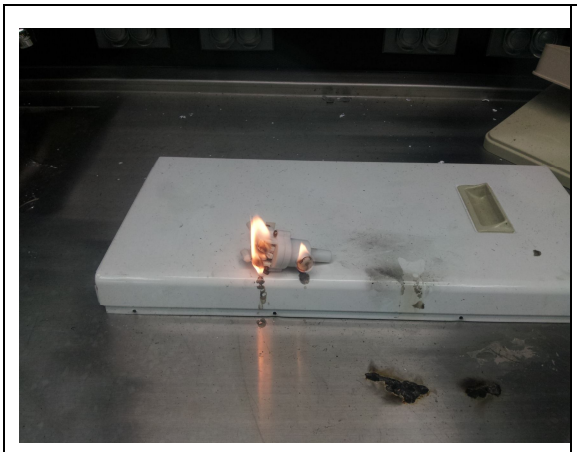
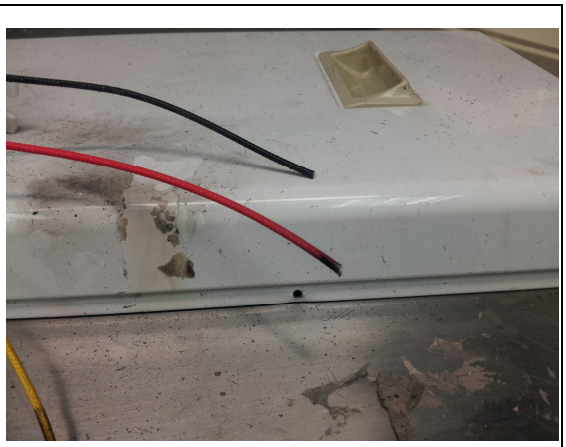
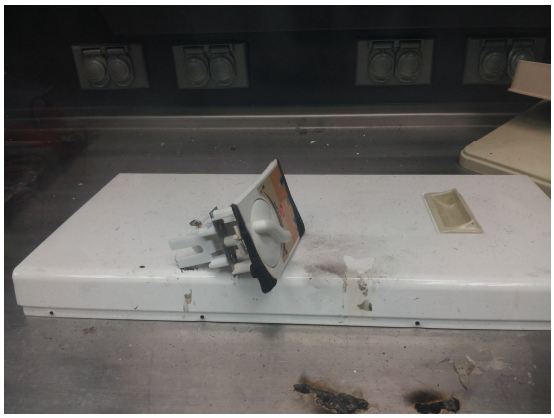
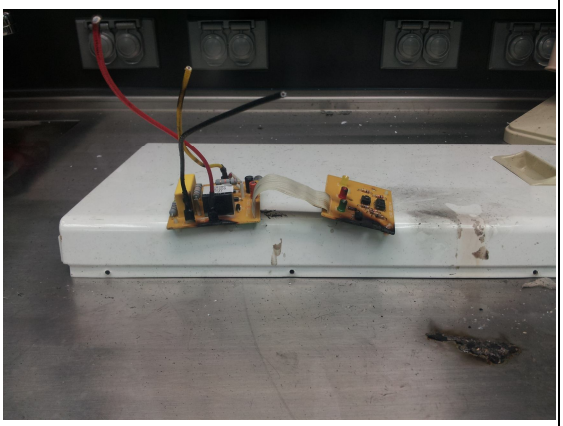


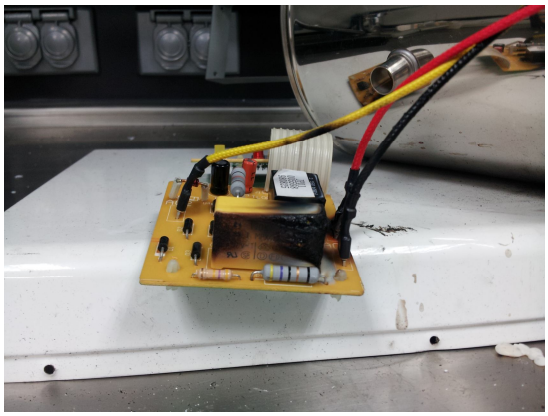
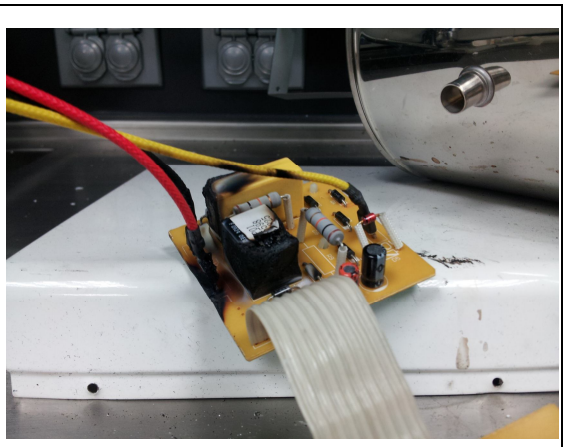
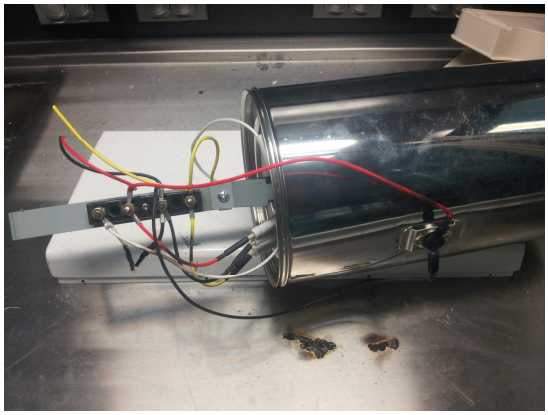
	

4.4 開飲機帶電部位進行燃燒試驗

對於 PCB 板、內部配線、電源線等電子元件，進行燃燒試驗。

表 4-6 開飲機帶電部位燃燒試驗圖

<table>
<tr><td>  </td><td>  </td></tr>
<tr><td>  </td><td></td></tr>
</table>

4.5 表格危險分析法-開飲機

使用表格危險分析法檢查開飲機在使用模式中或使用模式本身存在的危險，透過該方法全面、系統地識別潛在的危險源和危險狀態，分析發生危險的原因和危險後果及影響，預計這些危險對人員傷害或對產品破壞的嚴重性和可能性，進行定性風險評估，並提出相應的控制措施或緊急方案來消除或減少危險，以便在發生事故之前消除或盡量減少事故發生的可能性或降低事故有害影響的程度。

表 4-7 開飲機事故產品危險分析表

開飲機事故產品危險分析								
分析對象(層次)(1)						分析人員及日期(2)		
序號	分析項目	危險原因	危險	所處階段	危險影響	風險評估	建議措施	採取改進措施後的風險
1	塑膠外殼(前側)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
2	塑膠外殼(後側)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
3	塑膠外殼(底座)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
4	塑膠外殼(上蓋)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
5	熱水膽上蓋	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
6	矽膠管 1	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
7	矽膠管 2	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
8	矽膠管 3	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
9	矽膠管 4	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
10	矽膠管 5	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
11	生水阻隔開關(上)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
12	生水阻隔開關(下)	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
13	生水阻隔開關(蓋板)	不可燃物質	不燃燒	強迫著火	無	1E	無	
14	內部配線	不可燃物質	不燃燒	不著火	無	1E	無	
15	電源線	不可燃物質	不燃燒	不著火	無	1E	無	
16	水源開關	可燃物質	燃燒	強迫著火	環境破壞 人員傷亡	1D	添加阻燃劑	1E
17	塑膠溫膽	可燃物	燃燒	強迫	環境破壞	1D	添加阻	1E

		質		著火	人員傷亡		燃劑	
18	PCB 板	不可燃物質	不燃燒	不著火	無	1E	無	
19	電子元件(電容器)	不可燃物質	不燃燒	不著火	無	1E	無	
20	電子元件(繼電器)	不可燃物質	不燃燒	不著火	無	1E	無	
21	O-RING	可燃物質	燃燒	強迫著火	環境破壞人員傷亡	1D	添加阻燃劑	1E
22	端子座	不可燃物質	不燃燒	不著火	無	1E	無	

4.6 以 ETBA 進行分析分事故產品-開飲機

以電器產品而言，其本身在未供電時實為一不具任何形式能量的物體。當消費者將電源線插頭置入電源插座的那一刻，即將電能經由電源線導入，電能其路徑流過內部配線分別到達加熱環及控制電路板，期間亦流過相關產品保護元件裝置。電能轉換成熱能來使用，有熱就會有危險，熱能會導致塑料部件的老化脆化，而影響危險屏蔽之功能。值得探討的是，某些電子元件雖然其功能不是將電能轉化成熱能使用，但其使用時會有餘熱在其本身，導致該元件假使在耐受性或可靠性不足的情況下，有可能發生內部短路或其他未知因素將電能急速的轉化成熱能堆積在自身，進而引發火苗。在者，熱水膽上方的 O-ring 在使用一段期間後會老化脆化，導致水蒸氣之凝結水順著 O-ring 的破裂漏洞處流入開飲機內部，造成水可能直接接觸到相關代電部位，亦增加開飲機內部相對封閉空間的溼度，即影響到汙染等級可能造成原先安規所評估的空間距離及沿面距離不足的現象發生。

外物侵入的內部空間的因素也要一併考量，小蟲子或異物跑進開飲機機體內，碰出到帶電部位的正負極也有機會產生火苗。

因此，電能流入機體的路徑中，於哪些路徑流經相當 110V 的電壓之配件及零組件，於任何狀況短路時其電能將會轉化為熱能產生火

苗,如果沒有適當的能量屏蔽,將會造成進一步的強迫著火造成事故。

表 4-8　開飲機事故產品 ETBA 分析

能源	能源危險	危及目標	初始風險指數	屏蔽措施	最終風險指數	備註
熱能	電源線短路(被壓中勿)	可強迫著火部件	1D	待評估	1D	
熱能	繼電器內部接點老化	可強迫著火部件	1D	加裝鐵殼屏蔽	1E	
熱能	降壓電容器老化降低絕緣內部短路	可強迫著火部件	1D	加裝鐵殼屏蔽	1E	
熱能	異務侵入造成帶電部位短路	可強迫著火部件	1D	待評估	1D	
熱能	水滲入機體內部引起線路短路或受潮導致故障起火燃燒	可強迫著火部件	1C	於熱膽上設計水滴導流裝置且增設偵測器用以發出警告	4C	
熱能	熱膽於無水且保護裝置完全失效狀態下持續加熱	可強迫著火部件	1C	待評估	1C	

第五章 安全性調查結論與建議-開飲機

5.1 本安全性調查結論

事故的引發一般可歸納於三部份：人為疏失、設計不良及安裝不完善。以開飲機沒有安裝的過程而言，因此可直接探究人為疏失及設計不良這兩種因素。

開飲機常見的人為疏失不外乎是加水注入時超過滿水位線，水滲入機體內部造成觸電或短路故障；電源線被重壓導致電源線及插頭破損，該部位之阻抗增加造成溫升，甚至形成初期短路；開飲機屬高耗電之電氣產品，其它電器產品共用延長線時，功率過高亦容易造成事故。最後產品經常在使用一段時間後有輕微故障，但是經由非原廠檢修人員維修後使用非原廠規格的零組件，造成另外事故風險產生。

設計不良原由於採用品質不良的零件，或是大量生產時某些零組件因為缺料，緊急用其他不同規格的替代品裝設到產品上；採用塑膠材料的品質也需一併考量，由於開飲機產品之殼及內部構造絕大部份都是由塑膠(含矽膠)製成，於內部高溫環境下，對於塑膠造成的老化現象也是不可忽視的。

5.2 本安全性調查建議

於開飲機事故產品安全性調查下，發現產品本體結構採用大量塑膠材質來構成，而經由全面拆解燃燒測試後發現幾乎都是可燃的塑料居多。以 ETBA 分析法，首先要識別能量源由何處發起，接著識別屏蔽措施。

開飲機的火苗起源皆起於帶電部位或是相關零組件的老化異常，假使火苗的發生是無法完全消失的話，接下來要考慮的就是對其

屏蔽的路徑，如何使得塑膠無法強迫著火。依目前所知方法，可於塑膠部份添加阻燃劑使其無法強迫著火，如此即可作為良好的屏蔽措施。O-ring 及矽膠管部份於燃燒試驗時，為垂直狀態時為非常緩慢的速度延燒，如擺置為水平狀態時，一開始可以強迫著火，接著會以很慢的速度逐漸熄火，因此 O-ring 及矽膠管部份也建議加入阻燃劑以作為屏蔽措施，但其有飲用熱水流通過，是否 O-ring 及矽膠管部份加入阻燃劑後，會以化學反應污染飲用水或劣化其材質，是為可在深入探討的一環。

而市售開飲機於使用三四年後，熱膽上的 O-ring 老化脆化是相當普遍易見的，當水蒸氣的冷凝水或不當添加過滿的水經過劣化的 O-ring 低落於機體內部，造成內部空間之溼度增加，應該將安規內所限制的污染等級之考量提升至污染等級 3，才能有效提供帶電部件空間距離及沿面距離之保護。此外，亦可在熱膽本體上設計一額外的屏蔽方式，藉以導引水滴至機體外可有效降低前述所提的內部空間溼度。

目前針對市面上之事故產品，目前標準檢驗局之作法為再行取樣或購樣以相關標準進行安規測試，惟該作法無法識別有關產品材質結構老化因素，因此在事故產品分析中應加入安全性分析，藉以將相關建議有效的回饋到安全性驗證系統。

至於其他屏蔽方式的開發，仍可依事故產品發生的型態，對應其問題設計開發，期望能夠將事故發生率降至最低，有效保障生命財產安全。

參考文獻

[1] 陳凌峰，電氣產品安全原理與認證，人民郵電出版社，民國 97 年。。

[2] 趙延弟，安全性設計分析與驗證，國防工業出版社，民國 99 年。

[3] 姜同敏，可靠性與壽命試驗，國防工業出版社，民國 99 年。

[4] 謝里陽，可靠性設計，高等教育出版社，民 102 年。

[5] 王宏魯，電器保護組件化失效機理之基礎研究，經濟部標準檢驗局 101 年研究發展計劃。

[6] 張文昌，應用田口方法於產品失效鑑定，華梵大學工業管理碩士研究所論文，民國 94 年。

[7] 姚立真，可靠性物理，電子工業出版社 國 84 年。

[8] 劉明治，可靠性試驗，電子工業出版社 國 84 年。

[9] 王厚余，低壓電氣裝置的設計安裝和檢驗，中國電力出版社，102 年版。

[10] 李永華，燃燒理論與技術，中國電力出版社，100 年版。

[11] 付桂翠，電子元器件使用可靠性保證，國防工業出版社，民國 100 年。

[12] 柯煇耀，預防性失效分析，中華民國品質學會，民國 93 年。

[13] 楊善國，以預防保養為目的之失效分析與預測方法，國立交通大學機械工程系博士論文，民國 87 年。

[14] IEC 61508，Functional Safety of Electrical / Electronic / Programmable Electronic Safety – Related Systems，Geneve，1997。

[15] IEC 812，Analysis techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA)，Geneve，1985。

[16] Rausand, M. and Oien, K., "The basic concept of failure analysis", Reliability Engineering and System Safety,1996

[17] Rao, S. S., Reliability-Based Design, McGraw-Hill, New York, 1992.