系統保證於軌道工程之應用

新北捷運局副總工程司 / 林逸羣
中興工程顧問公司系統及電氣工程部計畫副理 / 吳培瑛
中興工程顧問公司系統及電氣工程部工程師 / 徐筱晴
中興工程顧問公司系統及電氣工程部工程師 / 卓悌琨

關鍵字：系統保證作業、RAMS 分析、軌道系統工程

一、前言

系統保證作業已廣泛應用於軌道系統工程，透過系統保證相關之分析與研究，將可確保軌道系統之可靠度、可用度、可維修度與安全度 (Reliability, Availability, Maintainability and Safety, RAMS) 能夠完整地納入軌道系統生命週期之中，並透過系統驗證與展現的作為，來證明建置之系統與設備，均能符合規範所要求的可靠度、可用度、可維修度與安全需求，使軌道系統在營運時，能符合整體營運之目標。

歐盟針對軌道運輸系統制定安全管理的規範，如 :EN50126、EN50128、EN50129 與 IEC61508 等，其中 IEC61508 為一通用的規範，適用於軌道運輸、航太工業、核能電廠及一般製造業；EN50126、EN50128 與 EN50129 則專為軌道運輸系統所制定，含括規劃設計、興建製造並延續至營運階段的所有安全規範，有關 EN50126、EN50128 與 EN50129 之範疇請詳圖 1。

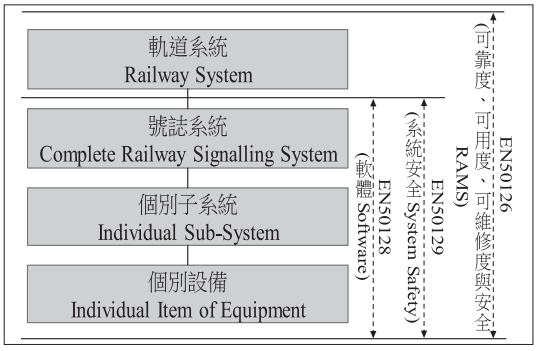

圖 1 EN5012X 之範疇

軌道工程之系統保證工作要求，係依據軌道運輸系統之國際規範，並透過邏輯化與系統化的方法來規劃與執行系統保證作業，展示業主所約定的功能均已充分地融入於設計中，並以各項積極性及預防性之安全管理過程，應用於工程建設的所有階段，以確保軌道系統在

營運時旅客、工作人員及大眾的安全。本文主要介紹系統保證作業所包含的要素、執行方法，與其在軌道系統中所扮演之角色。

二、定義

(一) 可靠度 (reliability)

依據 EN50126-1(3.30) 之定義，可靠度為系統在特定條件與既定時間內，成功執行所需要功能的可能性。

可靠度可分為固有可靠度 (inherent reliability) 與操作可靠度 (operational reliability)。固有可靠度為系統或裝備在假設的任務定義條件下所得到的可靠度值，僅含括產品設計與製造之綜合影響，可用於度量產品研製單位之研製可靠度水準，常被用於契約中定義產品的可靠度需求；操作可用度為顧客或使用者實際操作時所獲得的可靠度評估值，含括產品於設計、製造、搬運、環境、維護操作等綜合影響，可用於定義產品使用的可靠度需求，但一般而言不適合直接當作契約之可靠度需求。

為了明確判定系統或裝備的可靠度水準，可靠度必須以量化的數值加以規定，一般常用之度量指標如下：平均失效間格時間 (MTBF, 小時)、失效率 (失效次數 / 每百萬小時)、成功機率 (%) 等。

(二) 可用度 (availability)

依據 EN50126-1(3.4) 之定義，可用度為在所需要的外部資源均已獲得的情況下，產品在規定的條件下與規定的時刻 / 時間區間內處於可執行規定功能狀態的能力。

可用度分為固有可用度 (Inherent Availability)、達成可用度 (Achieved Availability) 與操作可用度 (Operational Availability)。固有可用度為在任何隨機時間 ，且理想的操作及支援環境條件下，產品被賦予任務時處於可用狀態的機率；達成可用度為在既定情況及想支援環境 (有效的工具、零件及人力等) 下，系統被賦予任務時處於可用狀態的機率；操作可用度既定情況及實際作業環境下，系統被賦予任務時處於可用狀態的機率。

(三) 可維修度 (maintainability)

依據 EN50126-1(3.20) 之定義，可維修度為在特定使用條件下，並按照規定的程序與資源執行維修時，在規定的時間區間內完成有效維修動作之可能性。

維修為使一系統或產品保持或恢復正常可用的狀況，所執行的一切措施。維修可分為：矯正性維修 (Corrective Maintenance, CM) 與預防性維修 (Preventive Maintenance, PM)。矯正性維修為針對系統與產品之失效所執行之一切非預定之維修行動，以恢復系統治所規定的工作狀況；預防性維修為保持一系統或產品在規定之工作狀況下，所採取的一切預防性維修行動，包含：定期檢驗、更換重要組件、校驗與保養等。

一般常見之可維修度度量指標包含：平均維修時間 (MTTR)、完成修復機率 (M(t)) 等。

(四) 安全性 (safety)

依據 EN50126-2(3.1.9) 之定義，安全性為免於不可接受風險的能力。

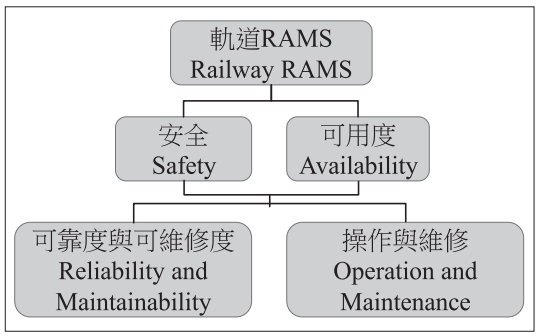

圖 2 EN50126 的 RAMS 架構

而系統安全 (System Safety) 為運用工程與管理的原理、原則、技術於系統 (產品) 生命週期各階段中，使得系統 (產品) 於有限的時間、成本、以及操作環境下獲致安全性的最適水準。

三、RAMS 組成要件

EN50126 說明於軌道系統中控制 RAMS 參數的方法，並述明 RAMS 的架構如圖 2，一般可依循此架構圖針對工程需求與發生的故障進行分類，以有效的與工程中各相關單位溝通。

軌道系統 RAMS 分為安全與可用度兩部分，當安全或可用度不符合需求時，均會影響整體軌道系統之 RAMS。而造成安全或可用度受威脅的原因，又分為系統可靠度與可維修度不足，或是營運與維修不良兩類原因。

當一個系統錯誤被判定是由於可靠度不足導致的，而與安全無關時，透過 RAMS 架構圖 (圖 2) 判斷此狀況將造成系統可用度無法達標。而可用度是由系統可靠度與維修度，以及營運與維護兩部分共同支持，此時若是透過加強營運與維修工作的方式，將有機會提升可用度直至符合標準，得以讓整體 RAMS 符合需求，此過程即為控制系統 RAMS 的手段。

四、RAMS 與服務品質的關係

RAMS 用以定義系統長期運轉的性能特性，須經由工程概念、方法、工具與技術，以保障於系統生命週期中，得以持續達成系統目標。RAMS 指標對於提供旅客的服務品質有直接影響，例如 : 列車準點率等。透過 RAMS 作業，於興建階段即可系統化的預估與展現軌道系統能否符合營運目標。

五、系統保證執行程序

依循 EN50126 訂定之生命週期 RAMS 相關工作項目，並綜整於軌道工程領域執行系統保證之經驗，繪製 RAMS 執行流程圖 (如圖 3 所示)，實際繳交之系統保證文件，仍依各工程案例規畫而定。

RAMS 活動涵蓋軌道工程之設計、施工、測試與驗收、試運轉與營運等階段，於每一階段結束前均應完成該階段應有之 RAM 分析、系統安全分析或驗證展現作業，並以文件之審查與確認，作為展現階段性成果及進入下一階段之憑藉。

為充分保證所執行工程之系統 RAMS，須先期規畫系統保證與系統安全計畫之執行標準、執行模式與應用規範，並遵循 EN50126 所律定之系統 V 型生命週期，訂定各階段工作應執行之系統保證作業。

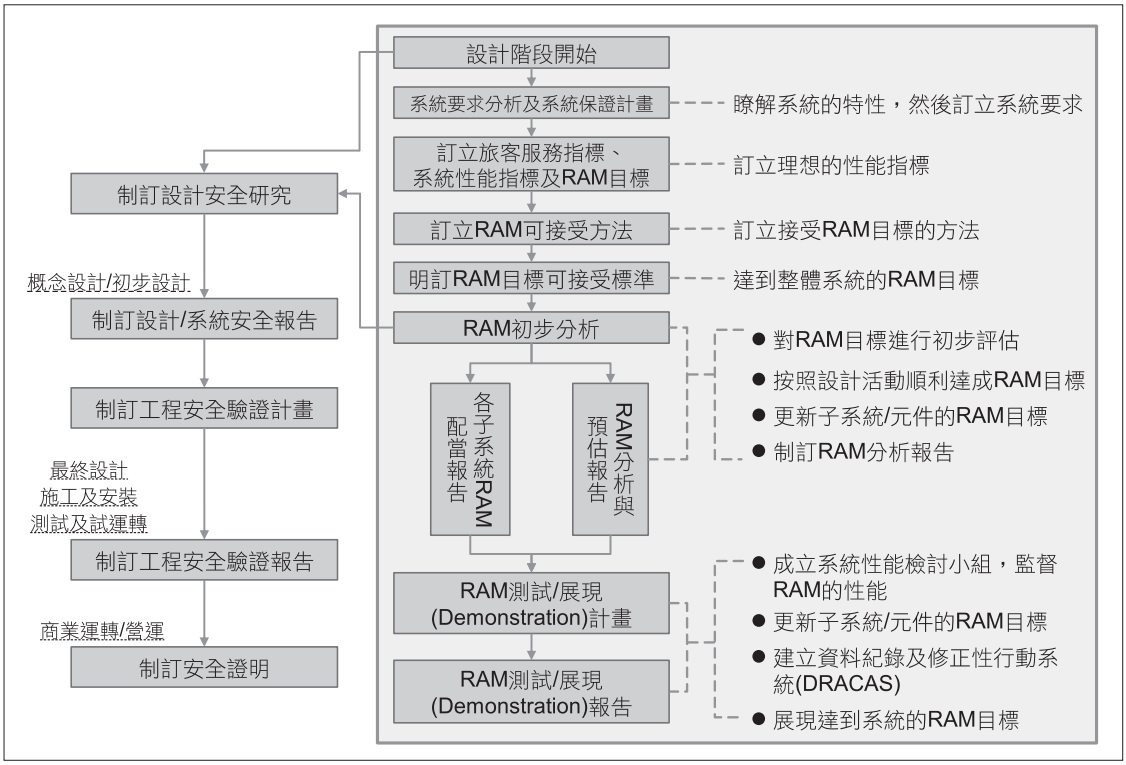

圖 3 RAMS 執行程序

系統 RAM 與安全需求之訂定，係依規範進行功能研究，並參考類似軌道系統依據所執行之工程系統特性進行需求分析，以完成系統 RAMS 需求訂定。

為符合系統 RAMS 需求，將於生命週期中依系統保證計畫，執行一系列 RAM 與安全分析作業，於設計階段針對設計內容，提出 RAM 預估報告以及設計 / 系統安全報告，並於測試階段執行工程安全驗證，以確認安全需求被確實執行，RAM 的作業成果，則透過 RAM 展現來驗證是否符合需求，詳細 RAMS 作業內容，將於後續內容呈現。

六、RAM 分析技術簡介

系統功能研究是 RAM 研究的基礎，在執行所規劃之各項工作之前，應先充分了解系統之設計原理、運作模式、組成元件及其間的功能關係。系統功能研究即透過設計圖審查，並將之轉換為系統功能方塊圖 (FBD)，透過串並聯的邏輯關係將系統功能由全系統階層向下細分至次系統、裝備甚至線上更換單元 (LRU) 階層，並賦予適當編號，以利後續 RAM 分析之用。

(一) 系統功能研究

RAM 分析模式的基本資料起始於系統功能方塊圖 (FBD)，此方塊圖描述系統中必要性能之次系統及其組件間之功能關係。RAM 分析模式即將此功能方塊圖重新轉換為另一種串並聯關係的網路中，以顯示各個次系統、裝備甚至線上更換單元間可靠度相關性，即可靠度方塊圖 (RBD)；可維修度方塊圖原則以可靠度方塊圖為基礎，考慮可維修之線上更換單元階層，假設所有可維修單元為串聯關係，由可靠度方塊圖予以轉換而得。

(二) 可靠度分析

參考前述可靠度方塊圖，再結合工作時間、失效率資料，評估系統的可靠度水準，此分析模式即可據以建立後續可靠度配當、預估分析之基礎。典型的可靠度分析模式可分為串聯系統 (Series System) 及並聯系統 (Parallel System)，茲分述如後：

1. 串聯系統 (Series System)：為最常用的可靠度分析模式，在串聯系統中必須每一個分系統均正常操作全系統才算正常。假設各分系統均互相獨立，則全系統之可靠度為各個分系統可靠度之乘積，亦即

$$R_s = R_1 \times R_2 \times \cdots \times R_n = \prod_{i=1}^{n} R_i$$

若每一個設備處於隨機失效期 (Random Failure Period)，或其失效時間分佈呈指數分佈，則系統可靠度為

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} \exp(-\lambda_i t) = \exp(-\sum_{i=1}^{n} \lambda_i t)$$

系統失效率為

$$\lambda_s = \sum_{i=1}^{n} \lambda_i$$

依據失效呈指數分配的假設，系統平均失效間隔時間 (MTBF) 為

$$\text{MTBF} = \theta_s = \frac{1}{\lambda_S} = \frac{1}{\sum_{i=1}^{n} \lambda_i}$$

2. 並聯系統 (Parallel System) ：為另一種常用的可靠度分析模式，在並聯系統中，只要有一個分系統正常，全系統即正常，也就是要每一個分系統都失效，全系統才算失效。假設各分系統均互相獨立，則全系統之可靠度為

$$R_s = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t})$$

其平均失效間隔時間 (MTBF) 為

$$\text{MTBF} = \theta_s = \frac{1}{\lambda_S} = \int_0^{\infty} R_s(t)dt$$

(三) 可維護度分析

可維修度分析之目的除滿足業主所頒佈之可維修度設計標準外，主要在於確定可維修度目標需求之展現，可維修度分析模式摘要說明如下：

1. 依據可靠度方塊圖轉換為可維修度方塊圖。
2. 依據可維修度方塊圖制定可維修件清單，即線上可更換單元 (LRU)。
3. 由可靠度預估結果獲得線上可更換單元零組件失效率。

4. 執行可維修度配當。
5. 制定線上可更換單元 (LRU) 之維修流程及步驟。
6. 執行可維修度預估 (含預防性保養需求、保養週期及備份件需求)。
7 確定可維修度需求目標滿足。

平均維修時間 (MTTR) 的計算方法有三，分別為直接算術平均數法、零件數作為加權之算術平均數法及失效率加權之算術平均數法。前二者是以修護單元及該單元的零件數做基礎，去分攤修復時間。但此二種算法所得之 MTTR 仍較不公平正確，故一般採失效率加權之算術平均數法，公式如下，其可較為準確計算設備之 MTTR 值。

$$MTTR = \frac{\sum_{i=1} \lambda_i \times MTTR_i}{\lambda_s} = \frac{\sum_{i=1} \lambda_i \times MTTR_i}{\sum_{i=1}^{n} \lambda_i}$$

其中，λ_i：各維修項目之失效率；
$MTTR_i$：各維修項目的預估維修時間。

(四) 可用度分析

於 EN50126 定義可用度為

$$A = MUT/(MUT + MDT)$$

其中，MUT：平均正常運轉時間 (Mean Up Time)，一般可用 MTBF、MTBSF 等表示；

MDT：平均中斷時間 (Mean Down Time)，一般可用 MTTM、MTTR 等表示。

於執行 RAM 預估時，一般以可靠度與可維修度之計算結果，採用固有可用度計算方式，其定義如下：

$$A = MTBF/(MTBF + MTTR)$$

七、安全分析技術簡介

「安全」一詞之意義為可免於各種不可接受之風險，如人員死亡、受傷、職業災害或設備及財產損失 ... 等事件。為保障乘客、員工與大眾於軌道系統營運與維修期間之安全，於軌道工程案例之設計、施工、測試與驗收、試運轉及營運等階段需求條款中，大多明訂要求承包商須執行系統安全計畫與相關分析作業，以確保軌道系統未來營運與維修期間將意外發生之機率降至最低，且將意外危害之嚴重性控制在最小的程度。一般來說，安全管理涵蓋危害確認、風險評估、風險控制等三個程序，詳細內容將於後續內容呈現。

(一) 安全分析方法

危害分析是安全管理的必要分析工具，從危害確認開始，進而分析事件發生的因果關係、評估事件造成的不良影響及發生機率。危害分析又可分為定性危害分析及計量危害分析，定性危害分析一般包括初步危害分析 (PHA)、次系統危害分析 (SSHA)、系統危害分析 (SHA)、操作及支援危害分析 (OSHA) 等；計量危害分析則包括缺陷樹分析 (FTA)、事件樹分析 (ETA) 及故障模式、影響及重要性分析 (FMECA)。

(二) IEC61508 定義之風險

IEC61508 將「風險」視為衡量危險的指標，此處之風險為危害發生的機率與嚴重性的組合，並定義下列四種風險：

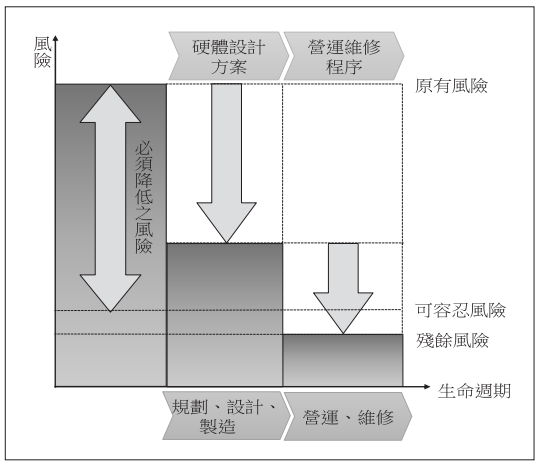

圖 4 IEC61508 降低系統風險的手段

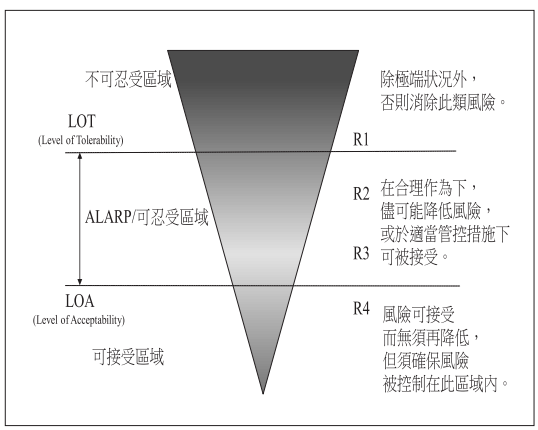

圖 5 ALARP 概念圖

1. 被控制的風險：只被控制裝置與裝置間互相作用產生的風險。
2. 可容忍的風險：在現行標準基礎下可以被接受的風險。
3. 殘餘風險：採取防護措施後仍殘留的風險。
4. 必須降低的風險：對安全相關系統進行需求分析及危害分析後，可得到系統的可容忍風險與被控裝置的風險 (現存風險)，兩者之差為必須降低的風險，管理者必須採取手段降低風險，使改善後的殘餘風險低於可容忍的風險。

一般而言，在建置階段會儘可能利用硬體的設計方案來降低風險，但若硬體設備的改善成本過高或技術無法達到時，則會進一步利用營運維修的程序來克服，直到系統剩餘風險低於可接受風險為止，請參考圖 4。

(三) 風險接受原則

於 EN50126 提到常用的風險接受原則，包含：英國 ALARP、德國 MEM 與法國 GAMAB，本文將以英國 ALARP 為例 (請參考圖 5)。

(四) 安全風險矩陣

為了有效控制風險，必須先建立一套評估風險等級的方法，所有經安全分析後的系統，均應作風險評量，確認其可能導致意外的風險等級。於 EN50126 提出構成風險矩陣的兩項主要因素，其一為危害的可能性或其發生的頻率，其二為危害所造成後果的嚴重程度。由前述兩項因素組成的風險矩陣表，提供安全管理過程中風險分級與評估重要基礎，並針對不同風險等級之危害訂定不同之處置方式，以有效的控制風險。本文提出案例供參考，請詳表 1 至表 4，仍應依工程對於風險之忍受特性，予以評估與調整後應用。

(五) 系統功能研究

系統功能研究是系統安全分析的基礎，在執行安全管理計畫所規劃之各項工作之前，應先充分了解系統之設計原理、運作模式、組成元件及其間的功能關係。系統功能

表 1 風險矩陣

嚴重程度 / 頻率 (次 / 年)		輕微 (S4)	不嚴重 (S3)	嚴重 (S2)	災難 (S1)
經常 (F1)	$F \geq 100$	R2	R1	R1	R1
有可能 (F2)	$100 > F \geq 1$	R3	R2	R1	R1
偶然 (F3)	$1 > F \geq 10^{-2}$	R3	R2	R2	R1
甚少 (F4)	$10^{-2} > F \geq 10^{-4}$	R4	R3	R2	R2
不大可能 (F5)	$10^{-4} > F \geq 10^{-6}$	R4	R4	R3	R3
不可能 (F6)	$F < 10^{-6}$	R4	R4	R4	R4

表 2 危害發生頻率分級

等級	頻率 F(次 / 年)	發生頻率說明
經常 (F1)	$F \geq 100$	可能會經常發生，可預料有關危害 / 失效將持續出現
有可能 (F2)	$100 > F \geq 1$	會發生多次，預料有關危害 / 失效會時常發生
偶然 (F3)	$1 > F \geq 10^{-2}$	可能會發生數次，預料有關危害 / 失效將發生數次
甚少 (F4)	$10^{-2} > F \geq 10^{-4}$	可能在系統壽限內，在合理情況下將預料有關危害 / 失效發生
不大可能 (F5)	$10^{-4} > F \geq 10^{-6}$	幾乎不會但有可能發生，可以假定只會在特殊情況下發生
不可能 (F6)	$F < 10^{-6}$	發生機會極微，可以假定危害 / 失效將不會發生

表 3 危害嚴重程度分級

等級	對人 / 環境的影響	對服務的影響
災難 (S1)	多人死亡 / 嚴重受傷 / 嚴重環境破壞	列車服務中斷 24 小時以上
嚴重 (S2)	一人死亡 / 嚴重受傷 / 對環境有相當程度的破壞	主要系統不能運作 / 造成系統服務中斷 1 小時以上
不嚴重 (S3)	輕微受傷 / 對環境有相當程度的威脅	系統嚴重損壞
輕微 (S4)	可能有人輕微受傷	系統輕微損壞

表 4 針對危害之處置

風險等級		定義
R1	不可忍受	必須消除該類風險。
R2	不理想	在一般情況下，必須將風險降低；只在沒有可行的風險減輕措施下，方可接受，需與業主達成協議。
R3	可忍受	可接受，但需有適當的管控措施並與業主達成協議。
R4	可忽略	可接受。

研究即透過設計藍圖審查，並將之轉換為系統功能方塊圖 (FBD) 及可靠度方塊圖 (RBD)，透過串並聯的邏輯關係將系統功能由全系統階層向下細分至次系統、裝備甚至線上更換單元 (Line Replacement Unit，LRU) 階層，並賦予適當編號，以利後續安全管理相關災害分析之用。

(六) 危害確認

配合實際工程進度，適時對工程所涵蓋範圍執行危害辨識及危害確認，危害確認將同時依據由上至下 (TOP-DOWN) 及由下至上 (BOTTOM-UP) 的分析程序，分別說明如後。

1. 由上至下 (TOP-DOWN) 分析程序

以基設階段所發掘及確認的初步危害登記冊 (Preliminary Hazard Log) 為基礎，檢視並篩選出屬於工程安全管理作業所涵蓋範圍之危害項目，進一步向下細分至工程安全管理相關之次系統或裝備層次，賡續執行後續危害評估、必要之危害控制及改正措施。

2. 由下至上 (BOTTOM-UP) 分析程序

為確保危害辨識及危害確認結果能涵蓋工程安全管理作業所有範圍，除前述由上至下 (TOP-DOWN) 手法所產生系統階層之危害項目外，同時須採用由下至上 (BOTTOM-UP) 的歸納方法，即經由裝備及次系統階層之設計審查，執行危害分析，如初步危害分析 (PHA)、次系統危害分析 (SSHA)、系統危害分析 (SHA) 及操作及支援危害分析 (OSHA) 等分析手法，進一步確認裝備及次系統階層的危害項目。

危害確認是危害分析的基礎，所有經辨識 / 確認的危害項目，應透過危害分析評估其風險等級、檢討危害減輕措施，登錄於「危害登記冊 (Hazard Log)」嚴密管制，同時透過 FRACAS 機制召集相關設計、製造及品保人員研討確認危害項目及減輕措施。

(七) 風險評估

1. 定性風險評估

透過次系統及裝備之設計審查，檢討類似次系統裝備曾經發生的危害事件、安全經驗、系統安全之設計理念，並運用危害分析之技術，檢視並確認該次系統或裝備是否也有相同的環境或發生類似危害事件的可能性。若有確認的危害項目，應評估其風險等級，並登錄於「危害登記冊 (Hazard Log)」嚴密管制。

2. 定量風險評估

危害事件經過系統安全定性分析後，確認其風險等級為不可接受時，且該系統為龐雜時，為深入了解其危險因子組合與發生機率，應進一步執行系統安全計量分析，提供設計者與決策者作更精準之判斷，確保安全管理能滿足系統之安全規格需求。常用之定量分析手法包括缺陷樹分析 (FTA)(如圖 6)、事件樹分析 (ETA)(如圖 7) 及故障模式、影響及重要性分析 (FMECA)。

(八) 風險控制

風險控制為安全管理之具體展現，一般係透過危害減輕措施達到風險控制的目的，危害減輕措施包含以下四種手法：

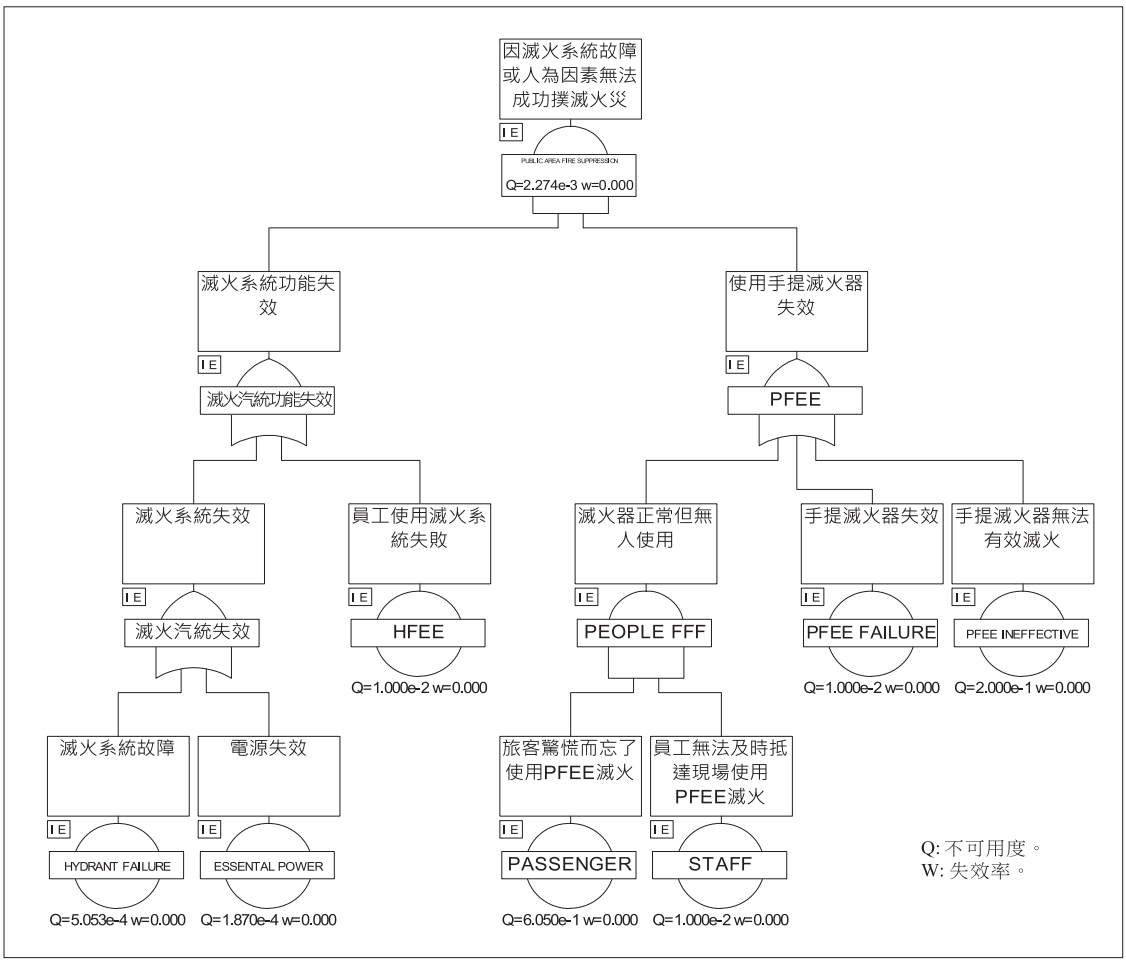

圖 6 缺陷樹分析 (FTA)

1. 設計修改。
2. 提供安全保護。
3. 增加警告裝置。
4. 建立特殊作業程序 / 訓練。

所有經危害確認項目均需透過風險評估程序評定風險等級，一般而言，評定為 R1 或 R2 風險等級的危害事項，必須盡快透過召開安全審查或類似功能會議，並檢視危害登記冊所列危害減輕措施，將風險減輕至 R3 或 R4 等級，只在沒有可行的設計辦法下，才可考慮營運、維修程序或為營運及維修員工提供訓練等方法來解決。

八、結語

系統保證作業為軌道工程必要執行的工作，其目的是以合理且有系統的方式分析系

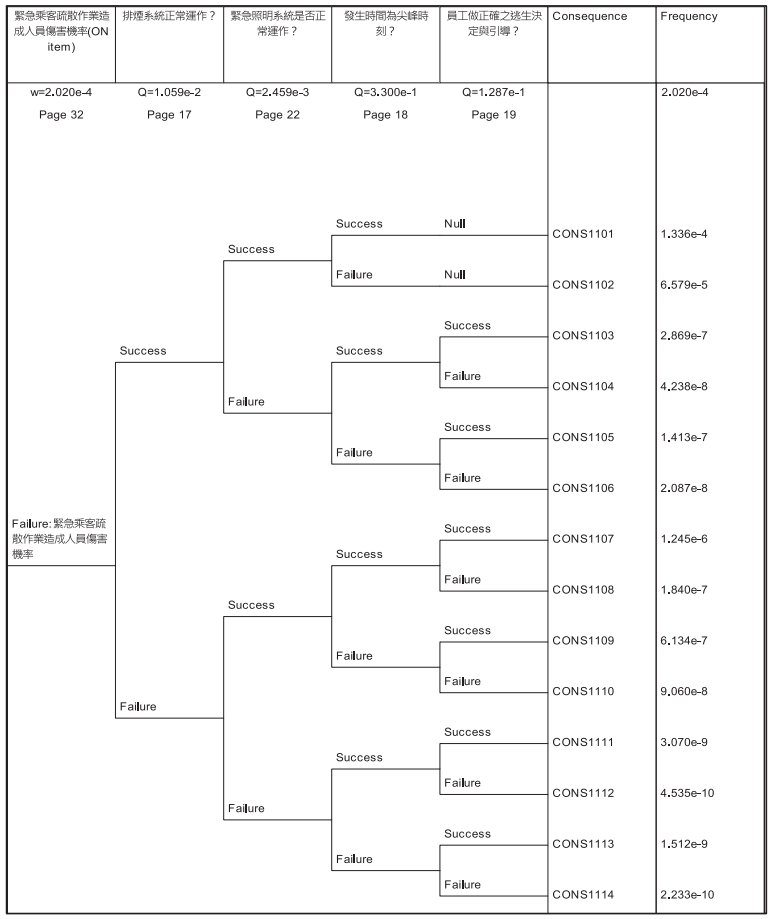

圖 7 事件樹分析 (ETA)

統可靠度、可用度、可維護度與安全，以保障軌道系統於未來營運時能夠達到工程所規範的 RAMS 目標，並確保系統運轉安全。

然而系統保證作業之執行成效，將取決於是否有完備的作業流程、正確的輸入數據與具豐富經驗的團隊執行。以統包工程而言，要實現系統 RAMS 目標除了需要考量採用高可靠度與維修度的設備 / 零件，同時必須強化對分包商與供應商的管控力度，並落實階段性的設計審查與系統保證作業稽查，除此之外，亦須投入資源於軟體工具、技術發展與失效資料提報、分析與改正系統 (Failure Report, Analysis, and Corrective Action System) 之維持等，此些作業恐將增加系統建置成本，為執行系統保證作業不得不面對的挑戰。

若於工程初期即開始執行系統保證作業，可即早確認系統 RAMS 性能，以防患於未然的精神，以期能降低生命週期成本。並

確保系統於未來營運階段，具有高可靠度、低維修工時與高可用度，且令風險得以被有效控制在合理可接受的程度。

參考文獻

1. Railway Applications-The Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), European Committee for Electrotechnical Standardization (CENELEC).
2. Railway Applications-Communication, Signalling and Processing Systems. Software for Railway Control and Protection Systems, EN50128, European Committee for Electrotechnical Standardization(CENELEC).
3. Railway Applications-Communication, Signalling and Processing Systems-Safety Related Electronic Systems for Signalling, EN50129, European Committee for Electrotechnical Standardization (CENELEC).
4. Quick Guide to the RAMS Standard EN50126/ IEC62278, Troels Winther.
5. 捷運系統安全管理探討， 中華顧問工程司。
6. 風險管理應用於鐵路運輸安全之初探 - 以台鐵風險分析與評量為例，交通部運輸研究所。
7. RAM 分析技術於捷運系統之應用，中興工程顧問。