機電系統工程之系統保證作業與實務

簡舜耀 [1]　許臨國 [2]

摘　要

系統保證是一種管理複雜系統之方法。應用於捷運系統中，大多數操作系統之系統保證專業技術，包括可靠度、維修度、安全、人因工程。因此系統保證專業分析是針對捷運系統之特性，進行評估與改良的一種工具，且爲整體系統保證計劃之一部份。本文就針對系統保證進行相關定義、作業流程，並佐以實例進行說明。

關鍵詞：系統保證、可靠度、維修度、可用度、系統安全、人因工程

Activity of System Assurance for E&M System Engineering

Shuen-Yau Chien　Lin-Kuo Hsu

Abstract

System Assurance is a methodology for management of complex systems. In the transit field, most operating systems employ a combination of reliability, maintainability, system safety, and human factors engineering in their system assurance applications. System Assurance discipline analysis techniques are tools for assessing and improving particular attributes of the transit system. The analyses are, therefore, an integral part of the system assurance program. This article introduces the definitions, operating procedures and application examples of System Assurance.

Key Words：System Assurance, Reliability, Maintainability, Availability, System Safety, Human factor Engineering

1. 臺北市政府捷運工程局機電系統設計處幫工程司　11166@trts.dorts.gov.tw
2. 臺北市政府捷運工程局機電系統設計處技正兼課長　10888@trts.dorts.gov.tw

一、前言

系統保證涵蓋四大領域，包括對於系統設備所指定的可靠度（Reliability）、維修度（Maintainability）、系統安全（System Safety）及人因工程（Human Factor）的需求，這四大領域一般統稱爲系統保證（System Assurance，SA）或 RAMS（Reliability, Availability, Maintainability, Safety）。

系統保證作業的目的在於確認該系統設備之故障週期、維修難易、潛在危險預防以及人性化程度能獲得保障。亦即：

(一) 提高可靠度

(二) 減少故障及維修所造成之營運中斷時間

(三) 降低營運及維修成本

(四) 所有經過確認的危險應予排除或降低其發生之風險

(五) 減少人機界面問題

二、定義

系統保證係以分析及驗證，就設備故障機率、保養維修難易程度、潛在危險之預防及控制能力，及人性化程度，來確保系統符合成本效益下之最大可用度及安全性；同時運用科學原理，來界定、預估、評析並加以控制系統可能的潛在危險。它以機率統計學爲經，參照相關系統及實務經驗爲緯，用來制定系統的可靠度需求、維修度標準，同時探討系統的安全性及是否符合人因工程。茲將系統保證領域常用之名詞及定義說明如后。

(一) 可靠度

可靠度即系統（或產品），在預定的使用年限及預設的工作環境下，能發揮足夠績效的條件機率；亦即發展一種新的或改進之產品，係使用操作需求建立最低允收之功能，以期待符合使用需求，其間各項因素（包括環境容許標準）之計算均會影響功能，藉計算所有可能失效以訂定合理之規範需求。

1. 關聯故障（Relevant Failure）

元件喪失其功能之關聯故障，係指經由下列原因，所造成之獨立故障：

(1) 在規定之設計及環境容許範圍內進行操作，所發生之元件故障。

(2) 依據廠商文件進行，而導致之不當操作、維修或測試，所發生之元件故障。

2. 非關聯故障（Non-relevant Failure）

不包含於關聯故障定義內，元件所發生之任何故障：

(1) 未能在指定之設計及環境容許範圍內操作，所發生之故障。

(2) 未依據廠商文件，而導致之人爲故障。

(3) 因其它設備功能失效所引起之故障。

(4) 因爲意外而非在元件正常操作下所引起之故障，例如軌道上有外物入侵或列車發生碰撞。

3. 平均故障間隔時間（Mean Time Between Failures，MTBF）

MTBF = T / n

T：同型元件累計之操作時間總和；

n：同型元件中發生關聯故障總次數

例如：

閉路電視系統總運轉時間在4,320小時內發生2次關聯故障，其平均故障間格時間爲4,320/2=2,160小時。

4. 失敗率（Failure Rate）

平均故障間隔時間之倒數，亦即關聯故障之頻率。

(二) 維修度

維修度（Maintainability），即一已失效系統（或產品），在允許停機時間及指定維修程序下，使系統或產品恢復功能的機率。

1. 預防維修（Preventive Maintenance）

系統、子系統、設備或設施依產品規範所擬定之計畫性維修週期所進行之維修作業，其包括保養與檢驗、組件整修，或對操作系統之功能查驗。

2. 校正維修（Corrective Maintenance）

將因爲非 產品規範所擬定之計畫性維修週期（不含天災意外或類似事件）所造成的系統、子系統、設備或設施故障，恢復至正常運轉狀態所進行之維修作業。

3. 平均修復時間（Mean Time To Repair，MTTR）

系統修護過程所需時間，MTTR = T / n

T：維修人員到達現場實際工作時間的總和，含發現故障原因、修理組件、拆除更新，及完成功能檢查，確認其恢復到可操作之狀態所需的時間。

n：T時間內關聯故障次數

例如：

閉路電視系統在運轉作業時間內發生2次關聯故障，而分別進行校正維修爲35分鐘與42分鐘，其平均修復時間爲爲（35+42）/2=38.5分鐘。

4. 最大修復時間（Maximum-Time-To-Repair，MTTR max）

所有校正維修時間某一百分準位（Percentile）之最大值，例如第90百分準位（90th percentile）意即必須有90%的校正維修時間小於此特定MTTR max90%值。

(三) 可用度

可用度（Availability），係指系統（或產品）隨時能使用的機率。系統經由最大化平均故障間隔時間，及最小化故障修復時間，以獲得高可用度。捷運系統自清晨 5 點發車前準備，到隔日凌晨 1 點收班，該系統應在這段時間內保有良好的可用狀態，其餘的時間可以用來進行定期維修保養。可用度常被定義爲實際的服務時間和要求的服務時間的比值，以百分比表示。本局木柵、內湖線因屬單一膠輪系統，車輛、號誌、供電等子系統密不可分，故以可用度衡量其系統穩定性，而高運量系統則以可靠度及維修度來評估系統穩定性及維修便利性。

1. 停機事件（Down Time Event）

(1) 停機事件，係造成系統延誤超過一行車間距（Headway）之任何降級服務，或中斷服務之故障。

(2) 延誤定義爲列車因故障造成之耽擱，亦即列車由一車站發車之實際時間與表排時間之時差。

2. 平均服務故障間隔時間（Mean Time Between Service Failures, MTBSF）

平均服務故障間隔時間，係指系統營運時數與停機事件次數之比值。

3. 平均復原時間（Mean Time To Restore, MTTR）

平均復原時間，係指所有超過一營運行車間距之延誤時間總和，與相對應之停機事件次數之比值。

4. 可用度（Availability）

可用度，係指平均服務故障間隔時間（MTBSF），比上平均服務故障間隔時間與平均復原時間（MTTR）之和。

5. 除外事件（Exclusions）

某些非系統本身的事件，亦可能造成延誤或故障。此類延誤或故障，毋須列入可用度之計算，下列爲此類狀況：

(1) 旅客造成之系統中斷（除非歸因於車門故障，而造成其他車門超載及壅塞，或者旅客因系統相關狀況之反應，而造成之延誤或故障）。

(2) 未經許可而闖入系統之人、動物，或物件所造成之中斷。

(3) 非系統本身所造成之服務中斷。

(4) 正常營運期間，超出環境特定限制。

(5) 破壞。

(四) 系統安全

系統安全係將各種知識與資源加以整合利用，以避免系統在整個生命週期中發生危險，亦即用以表示相對性地免於傷害或機率較低等可接受程度的風險。

1. 危險（Hazard）：

一種會導致潛在傷害、死亡或設備損壞之狀況。

2. 初期危險分析（Preliminary Hazard Analysis，PHA）：

是一種功能性之危險分析，用以有系統地定義及評估各種可能會影響系統操作安全的各種狀況。

3. 子系統危險分析（Subsystem Hazard Analysis，SSHA）：

針對子系統內可能會影響系統操作安全之各種狀況所進行的系統性記錄評估。

4. 系統危險分析（System Hazard Analysis，SHA）：

針對設備於測試、操作或維修時所需之作業進行系統性之審查與評估，用以判斷何種情況可能導致受傷、死亡或設備損壞。

5. 操作危險分析（Operational Hazard Analysis，OHA）：

是一種功能性之危險分析，用以有系統地定義及評估各種可能會影響系統操作安全的各種狀況。

(五) 人因安全

人因工程：旨在「發現關於人類的行爲、能力、限制和其它特性等知識，而應用於工具、機器、系統、任務、工作和環境的設計，使人類對於他們的使用更具生產力、安全與有效果。」

1. 人機系統：

一種或多種實體間之互動關係，以給定的輸入產生想要的輸出（目標）。

2. 人體工學：

人體工學係指研究人體活動與空間之間的正確合理關係，以求人在空間中最有效率的生活機能表現。

三、系統保證作業流程

系統保證應用於捷運機電系統中，包括可靠度、維修度、系統安全、人因工程。因此系統保證即爲一種針對捷運系統特性 ，進行評估與改良的工具，且爲整體系統工程之一部份。茲將本局機電系統保證作業流程，概述如後。

(一) 可靠度

1. 招標階段

在特別技術規範中訂定可靠度需求。

2. 細部設計階段

廠商依據可靠度設計準則，提送子系統流程圖、可靠度方塊圖、可靠度配當、故障模式、效應與嚴重性分析等文件。

3. 驗證階段

在系統開始營運後，進行可靠度驗證測試，廠商應先提送驗証之時程、程序、成功／失敗之標準、失敗之補救措施，及記錄報告格式等。

(二) 維修度

1. 規劃階段

在特別技術規範中訂定維修度需求。

2. 細部設計階段

廠商依據維修度設計準則，提送預防維修、校正維修分析等文件。

3. 驗證階段

可靠度／維修度驗證，係用以確認系統及各子系統，是否符合契約可靠度/維修度需求。測試計畫應於開始驗證前擬定，包括下列各項：

(1) 驗證目的。

(2) 驗證所需之設備及數量。

(3) 驗證時程。

(4) 驗證方法，包括維修人員於驗證時所應具備之技術水準。

在驗證期間，維修人員依據維修手冊，施以預防維修及校正維修，並填具運轉時數、維修故障資料，同時參加可靠度／維修度驗證測試審查委員會，討論驗證結果。

4. 故障審查委員會（Failure Review Board，FRB）

故障審查委員會成立目的，在於審查可靠度／維修度驗證之關聯故障、非關聯故障、維修狀況、以及確保在驗證階段，採取適當之維修作業並予以記錄。

故障審查委員會應審查有關系統功能／績效之故障資料，該故障資料係取自於可靠度／維修度驗證結果。所有故障資料必需提送故障審查委員會審查，該故障資料應包含故障發生時之操作狀況、故障發生之徵兆、故障隔離程序、已知或可能之故障原因。上述未解決之項目將追蹤列管，直至已圓滿確認出故障情況，並採取適當之修正作業爲止。

故障審查委員會之作業記錄應予歸檔，以利契約期間查核之用。故障審查委員會由捷運局設計單位、系統保證小組、工程處、工務所、捷運公司、廠商等各領域之適當人員所組成。

(三) 可用度

1. 規劃階段

招標階段，在特別技術規範中訂定可用度需求。

2. 細部設計階段

廠商應就會影響可用度之各子系統設備及元件，進行可靠度及維修度分析，分析應就會影響可用度之各子系統設備及元件，說明：

(1) 功能描述，包含子系統概要圖及功能流程圖。

(2) 可靠度方塊圖。

(3) 可靠度配當。

(4) 各項故障檢修所需之人時。

3. 驗證階段

在系統開始營運後，進行可用度驗證，廠商應先提送驗証之時程、程序、成功／失敗之標準、失敗之補救措施，及記錄報告格式等。

(四) 系統安全

系統安全作業係爲減少或消除系統在研製、儲運及使用過程中發生危害事件的工作項目。其目標無非減少由於意外事件對系統造成傷害或損失、防範人員傷亡及避免損傷其它裝備。其做法可藉由最低危險設計、安全裝置、警告裝置及特殊程序獲得解決。

造成危險的因素可分爲人爲疏失及設備故障，引此藉由相關安全設計準則可將危險予以排除。

1. 設計準則：

(1) 危險評估

建立危險之嚴重性分類，以針對因爲人員疏失、環境不良、設計不佳、程序缺失、以及系統、子系統、零組件故障或誤動作・・・等所導致之最壞可能結果，提供一定性化之評量。

(2) 捷運系統之危險分類如下：

第1類：致命（Catastrophic）危險

A. 對系統目標之影響——運輸系統停頓，無法完成任務。

B. 對營運能力之影響——系統之任何部份皆無法搶救，全數報廢。

C. 對安全／人員之影響——員工與（或）乘客死亡或多人受傷。

第2類：重大（Critical）危險

A. 對系統目標之影響——運輸系統嚴重損壞，需依輔助方式完成任務。

B. 對營運能力之影響——運輸系統中兩個或以上之主要子系統損壞，且此種狀況在現場無法於一小時之內修復。

C. 對安全/人員之影響——員工與（或）乘客因爲從事系統操作與維修、搭乘系統或因位於系統附近區域而受傷。

第3類：邊際（Marginal）危險

A. 對系統目標之影響——運輸系統可因爲利用待命之複置操作選擇模式而達運轉目標。

B. 對營運能力之影響——超過一組元件或子系統損壞，且此種情況在現場於一小時之內可以修復或置換者。

C. 對安全／人員之影響——員工與（或）乘客受傷。危險情況可經由自動裝置、警告裝置或特別操作程序・・・等加以控制。

第4類：可忽略（Negligible）危險

A. 對系統目標之影響——對系統運輸無任何可衡量之影響。

B. 對營運能力之影響——對運輸系統無明顯之損害。

C. 對安全／人員之影響——員工與（或）乘客無人受傷。

2. 系統安全分析：

系統安全分析可分初期危險分析、子系統危險性分析、系統危險性分析、操作危險分析進行，如下所述：

(1) 初期危險分析（Preliminary Hazard Analysis，PHA）

初期危險分析係於設計階段時進行，並且成爲日後分析之基礎文件。本分析係針對因爲整合各子系統所產生之前在危險，所進行的研究作業。

(2) 子系統危險分析（Subsystem Hazard Analysis，SSHA）

子系統危險分析之進行係對每一子系統之潛在危險提供分析，並涵蓋與系統安全有關故障所進行之研究。

(3) 系統危險分析（System Hazard Analysis，SHA）

系統危險分析之目的係針對用以判斷與子系統整合／界面有關之危險。

(4) 操作危險分析（Operational Hazard Analysis，OHA）

操作危險分析可對測試、操作與維修設計、程序及手冊等提供輸入，本分析將成爲教育訓練之主要輸入，使資源可配置於最大利益處。

(5) 重大／致命項目列表（Catastrophic /Critical Item List，C/CIL）

A. 重大／致命項目列表係針對於PHA、SSHA、SHA、OHA所確認之第1及第2類危險加以編列。

B. 重大／致命項目列表之目的在於其對主要危險之追蹤、解決與控制。重大／致命項目列表開始於最後之設計階段而持續至營運時期，此種重覆性的過程將持續直至所列項目皆被解決爲止。

3. 危險解決：

完成危險評估程序後，即可考慮是否接受危險帶來的危險，或決定去除或控制危險。相關人員可採取各種方式將危險帶來的危險降低至管理階層可接受的程度。以下步驟依照優先順序列出一些可採用的解決方法或措施將危險予以排除。解決危險依序之四個步驟：

(1) 最低危險設計：在系統發展過程中主要考慮的是必須選取適當的設計特性，以確保其固有之安全。(例如：散熱裝置、電路保護（熔絲）、等考量)，範例如圖1。

(2) 安全裝置：對已知而無法經由設計選取而排除之危險，必須採用適當的安全裝置，以將該危險排除或控制至可接受之水準。(例如：防愚裝置，號誌CSEX Board電路板插座設Key，若電路板與插槽不能相配（Match）則無法插入)，範例如圖2。

(3) 警告裝置：對於已確認之危險，若不可能排除其出現或發生，則必須採用特殊裝置以利異常狀況之及時偵測及產生適當的警告訊號。(例如：張貼警語、反光貼紙、警示音、警示燈)，範例如圖3。

(4) 特殊程序：在不可能經由設計或使用安全與警告裝置而降低其危險的地方，則必須發展特殊之程序及（或）預防性指示。(例如：設備操作、維修手冊)，範例如圖4。

4. 實例分析：

(1) 危險解決實例（四大步驟範例)：如圖 1至圖 4所示。

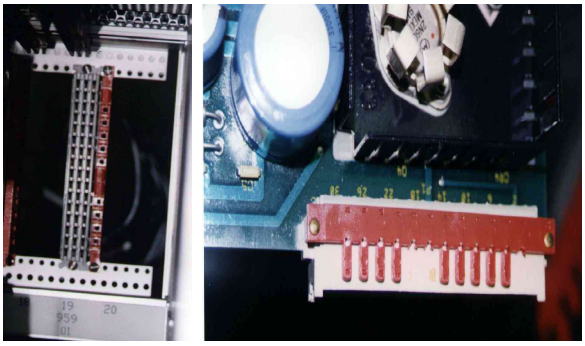

圖 1　最低危險設計－防愚安全裝置

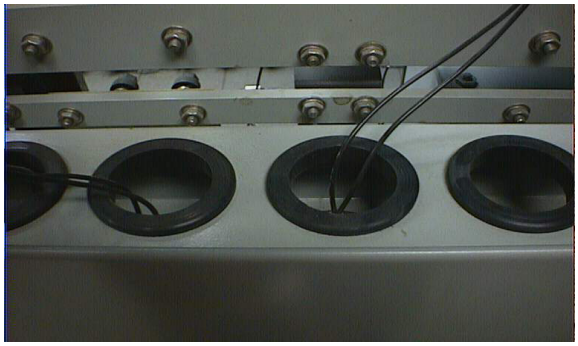

圖 2　安全裝置－保護線纜避免割傷

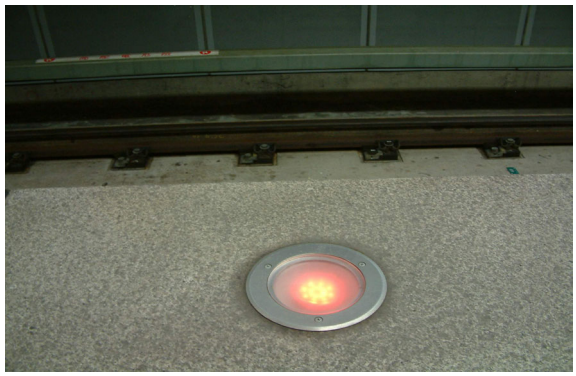

圖 3　警告裝置－月臺警示燈

(2) 號誌部份

如圖5所示，隧道內，就管線加裝斜板（Ramp）及蓋板（Cover)，並於斜板之板面兩側張貼反光貼紙以利人員辨識，另覆蓋板（鍍鋅鐵板）之表面應具止滑功能（廠商採用花紋粗糙面）且兩端邊緣無利邊處理，以避免人員因接觸遭受傷害。

圖 4　特殊程序－張貼警告標語

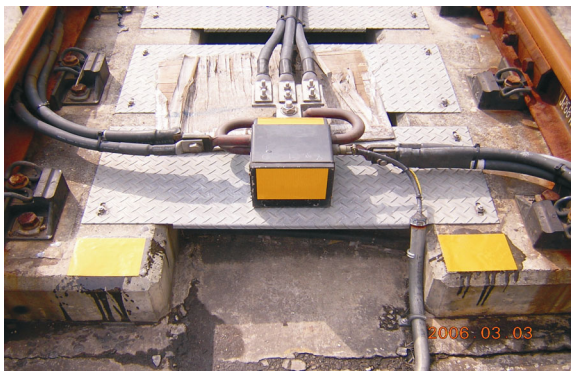

圖 5　斜板（Ramp）板面兩側張貼反光貼紙

(3) 月臺門部份

捷運系統講求安全、迅速、舒適度及便利性，降低環境空氣污染，以安全爲首要，攸關乘客性命，因捷運系統在自動控制系統操作下，爲防止意外發生，故規設防護設施，有加裝月臺門設置之考量。月臺門系統最大優點在於提高捷運系統乘客在月臺候車時的安全性，可避免乘客跌落軌道，或阻止蓄意侵入軌道人員。爲防止意外發生，平常無列車進站時月臺門爲關閉狀態，當列車進站抵達且定位停妥後再將車門與月臺門依系統設定方式開啓，當列車離站時再依系統設定方式關閉車門及月臺門；並設計有手動及自動啓閉開關裝置。月臺門上方設有月臺門關門警示燈，警示燈閃爍時，表示月臺門即將關閉。當旅客攜帶物品或身體部位被夾住時，列車車門/月臺門，設有防夾重開裝置，可防止意外夾傷，如圖6所示。

圖 6　月臺門及關門警示燈

(4) 供電部份

A. 第三軌保護：如圖7所示，於第三軌加裝保護蓋，標記高壓危險警語。

B. 礙子的裝置：如圖8所示，於第三軌支架與第三軌間，加裝絕緣礙子。

圖 7　第三軌保護蓋

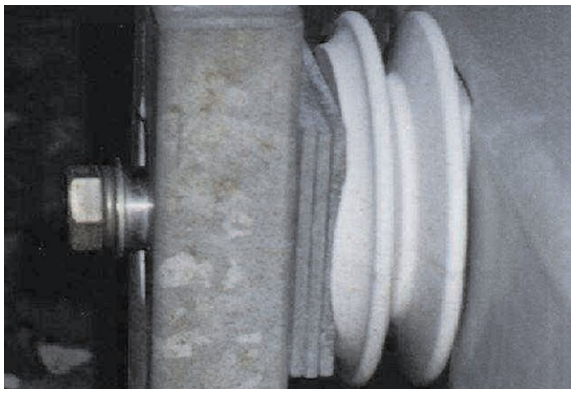

圖 8　礙子絕緣保護裝置

(5)通訊部份

A. 月臺婦女保護區

據1999年3月31日中時晚報報載，捷運公司爲保護婦女人身安全特於捷運雙連站於月臺設置婦女保護區，並加設攝影機監視該區域婦女同胞以防不明人士騷擾時能緊急處理。婦女保護區之範例如圖 9所示。

圖 9　月臺設置婦女保護區

B. 網路與防火牆安全

(A) 存放機密性及敏感性資料之大型主機或伺服器主機（如Domain Name Server等），除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身份辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取（如一般網路服務文件傳輸協定HTTP（hypertext transmission protocol）、遠程載入工具Telnet、檔案傳輸協定FTP（File Transfer Protocol）等的登入密碼），及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

(B) 爲提升大型主機或伺服器主機連線作業之安全性，應視需要使用電子簽章及電子信封等各種安全控管技術，以建立安全及可信賴的通信管道。

(C) 與外界網路連接的網點，應加裝防火牆，以控管外界與內部網路之間的資料傳輸與資源存取。

(D) 防火牆應具備網路服務的轉送伺服器（即代理伺服器，Proxy Server）以提供Telnet、FTP、WWW、Gopher等網路服務的轉送與控管。

(E) 網路防火牆的安裝與網路架構之規劃及設置，應依機關訂定的資料安全規定及資料安全等級分類，以最經濟有效的方式配置。

(F) 防火牆應由網路系統管理人員執行控管設定，並依機關制定的資訊安全規定、資料安全等級及資源存取的控管策略，建立包含身份辨識機制、來訊服務（incoming service）、去訊服務（outgoing service）與系統稽核的安全機制，有效地規範資源被讀取、更改、刪除、下載或上傳等行爲以及系統存取權限等資訊。

(G) 網路系統管理人員應由系統終端機登入防火牆主機，禁止採取遠端登入方式，以避免登入資料遭竊取，危害網路安全。

(H) 防火牆設置完成時，應測試防火牆是否依設定的功能正常及安全地運作。

(五) 人因工程

人因工程作業在於確認該系統設備之故障週期、維修難易、潛在危險預防以及人性化程度能獲得保障。

1. 設計原則：

(1) 手控設施設計原則

A. 功能相關的控制器應配置在一處，不同的控制器應易於分辨。

B. 控制器的選擇須配合四肢的特性。

(2) 視覺設施設計原則

A. 依判讀距離設計大小、排列、距離、顏色與光澤。(字體顏色與背景有別，字型不宜花俏)。

B. 配合觀測之方向安排角度，重要儀表應位於視界中央。

(3) 聽覺設施設計原則

A. 頻率在200-5,000赫茲（Hz）間最適宜。

B. 音調應與一般有別（警音與提示音)。

C. 避免與其它音響訊號雜音混淆（在播音時，背景音樂可主動降低分貝)。

2. 實例分析：

(1) 消防隊無線電連接插座（Fire Service Department）

目的：透過消防單位之主控車與本裝置的連結提供消防人員處理捷運系統在地下、隧道段處理事故之通訊界面，設計範例如圖10及圖 11所示。

人機界面注意事項：

A. 該洩漏電纜的裝置設計要能便於使用者收取便利。

B. 箱體本身須有IP55工業防護等級之防塵、防水設計。

C. 箱體內、外框無利邊，避免割傷電線電纜。

D. 外殼採用不銹鋼及銘牌顯示。

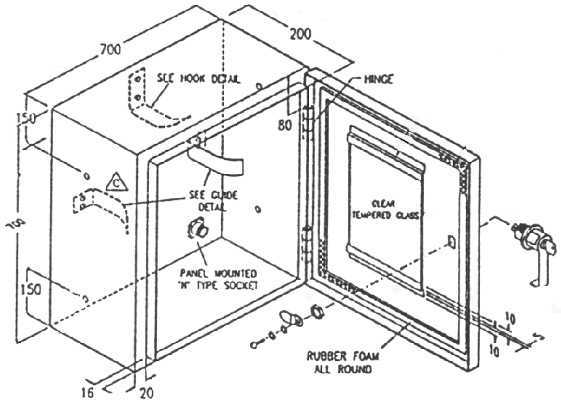

圖 10　消防無線電連結插座圖

圖 11 消防無線電連結插座外觀圖

(2) 月臺之閉路電視監視系統

目的：提供列車駕駛員透過攝影機所攝入之月臺區影像將之顯示於月臺監視器輔助駕駛員察看列車外圍之人群動態。

人機界面注意事項：

A. 高架段須考慮日曬因素會造成監視器，設計範例如圖12所示。

B. 地下段須考慮列車進站前，避免造成列車燈光的照度變化對於攝影機的影響，故採用對逆光補償較佳之攝影機

圖 12　月臺監視器實圖

克服光害。

四、結語

捷運系統的興建，爲能提昇機電系統之可靠度及維修能力，因此設有系統保證，除了在一般設計審查，及品質保證部門外，能從另一角度審查評估整個機電系統，亦即在機電招標、設計、測試等階段，進行有關可靠度、維修度等作業。

依英國軌道科技策略中心（Railway Technology Strategy Center, RTSC）所成立 Community of Metro 及 Nova 組織統計顯示，2003 年「兩事件（延誤 5 分鐘以上）間車廂千公里數」，台北捷運與世界各地十餘個地區捷運相較高居第二名，僅次於東京地鐵，這亦是有效發揮可靠度、維修度作業之例證。

所以除了土建與機電密切配合，設計與驗證亦需相互呼應，台北捷運才能達成世界級之水準，藉由系統保證的基本理念提供設計與審查者一參考方向，藉助此觀念在友善的界面設計中獲取舒適、安全、可靠、易維修的系統。

參考文獻

1. 《捷運機電系統工程系統保證計畫書廠商指南》。

2. 許臨國（1993）：「系統保證」，《臺北市政府捷運工程局機電系統訓練課程講義》，1993 年 5 月。

3.〈南港線通訊、號誌標廠商送審細部設計審查文件〉：

(1)“FSD RADIO ACCESS BOX LAYOUT”，機電系統設計處型管文號：（CIN：M50696, M52026, M53402,M60088）。

(2)“ERGONOMIC REPORT - HARDWARE”，機電系統設計處型管文號：（CIN：M62395）。

4. 簡舜耀（1995）：「人因工程實務演練」，「可靠度及人因工程實務專題班教材」。