高可靠度三重容錯數位儀控技術

High Reliability Digital Instrumentation and Control Technique for Triple Modular Redundancy Fault Tolerant Controller

徐獻星、陳昌國

Shian-Shing Shyu, Chang-Kuo Chen

數位儀控系統已廣泛應用於工業控制，利用數位電腦之通訊及自我診斷等優勢，可配置成多重容錯架構，在電子組件故障或受環境因素造成單機失效時，能以多數決之方式，維持控制器之設計功能。本文說明國際間著名之三重容錯控制器設計概念，並介紹國內發展三重容錯控制器之進程。

Digital instrumentation and control (DI&C) systems have been applied in industry widely. Taking the advantages of communication and self-diagnostic capabilities of digital equipments, they can be configured as a redundant control system to maintain application's design function by voting mechanism when single equipment malfunction occurs owing to environmental effect or component failure. This paper presents designs of several triple modular redundant (TMR) controllers used worldwide and the development of a TMR controller by domestic effort.

一、前言

早期安裝在工業控制設備，譬如發電廠及化工程序之控制系統，多半以類比系統為主，雖然這類系統可以有效地提供監測和控制功能，但受到過時 (obsolescence) 組件的影響，已逐漸由數位控制器所取代，譬如微處理器 (microprocessors)、可程式邏輯控制器 (programmable logic controller, PLC) 以及分散式控制系統 (distributed control system, DCS) 等。且利用數位電腦之通訊及自我診斷等優勢，可配置成多重容錯架構，在電子組件故障或受環境因素造成單機失效時，能以多數決之方式，維持控制器之設計功能。

針對數位系統，功能安全 (functional safety) 國際規範標準 IEC 61508[(1)] 指出，安全功能取決於一個系統或者一個組成元件在輸入訊號之後是否能正確地運作，是整體安全的一部分，並定義了四個安全完整性等級 (safety integrity level 1－4, SIL 1－4)，等級越高代表可靠度越高。安全完整性可以透過安全失效分數 (safe failure fraction, SFF) 與硬體容錯裕度 (hardware fault tolerance, HFT) 求得。SFF 表示系統硬體組件之可偵錯度，SFF 的值越高，代表系統處於風險的機率越低。HFT 代表系統硬體可允許之失效個數，譬如三選二之三重容錯架構其 HFT 為 1 (二選一之雙重容錯架構其 HFT 也為 1，但雙重容錯架構其可

安全失效分數 (SFF)	硬體容錯裕度 (HFT)		
	0	1	2
< 60%	不允許	SIL1	SIL2
60% －< 90%	SIL1	SIL2	SIL3
90% －< 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

表 1.
安全相關系統最大允許的安全完整性。

靠度較三重容錯架構差)。表 1 說明安全相關系統最大允許的安全完整性，明顯地，同等級的 SFF，若 HFT 越高，相對應的安全完整性也越高。國際間通過 IEC 61508 SIL3 認證之控制器包括 Tricon[2] 與 HFC-6000[3]，皆為三重容錯架構。

雖然國內儀控系統技術發展長期著重於工業運用，但因關鍵性組件控制器仍有賴國外進口與安全性需求的限制，使國內儀控技術無法有效應用於需求高可靠度之相關產業。因此，為了建立自主型儀控技術的目標，促進國內高可靠度儀控產業發展，並推廣至相關產業應用。核能研究所 (Institute of Nuclear Energy Research, INER) 提出台灣核能儀控系統 (Taiwan's Nuclear I&C System, TaiNICS) 專案，為一個具多方向的長期發展計畫，包括建立具高可靠度之數位控制器、軟硬體測試與驗證、儀控系統設計以及系統安全分析等，目標為應用於核能發電廠或化工廠中具高可靠度需求的系統。

TaiNICS 專案建立具高可靠度數位控制器之途徑，係基於台塑公司已發展成熟的工業級控制器 FCS-2000 (Formosa Controller System)[4]，開發具三重容錯架構之新型控制器 (NCS-1000)，原型設計如圖 1 所示，主要執行對策為：

1. 輸入訊號 (input signal)：透過輸入感測器或量測裝置，提供三重容錯數位控制器輸入訊號。
2. 輸入處理 (input process)：在進行邏輯執行前，於每個數位控制器內執行三選二投票邏輯，避免因電子組件故障或受環境因素造成的單機失效。
3. 邏輯執行 (logic execution)：執行三重容錯數位控制器內部邏輯程式，並將結果提供給輸出模組驅動輸出裝置。
4. 輸出處理 (output process)：負責驅動輸出裝置，可利用硬體邏輯，譬如繼電器組等，執行三選二投票邏輯，避免單機失效。
5. 控制器通訊 (inter-controller communication)：以專線連接三台控制器，進行偵錯診斷數據傳輸。

本文分別以第二章及第三章，介紹上述 Tricon 與 HFC-6000 兩類控制器之重要特性，並說明國內

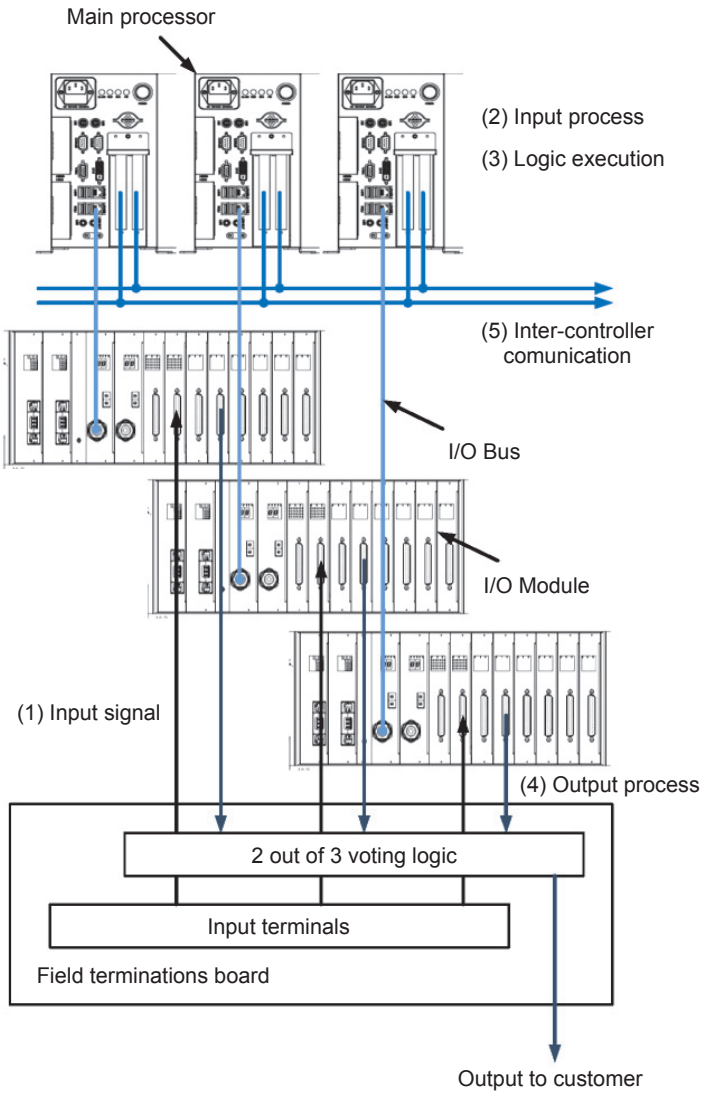

圖 1. NCS-1000 原型設計。

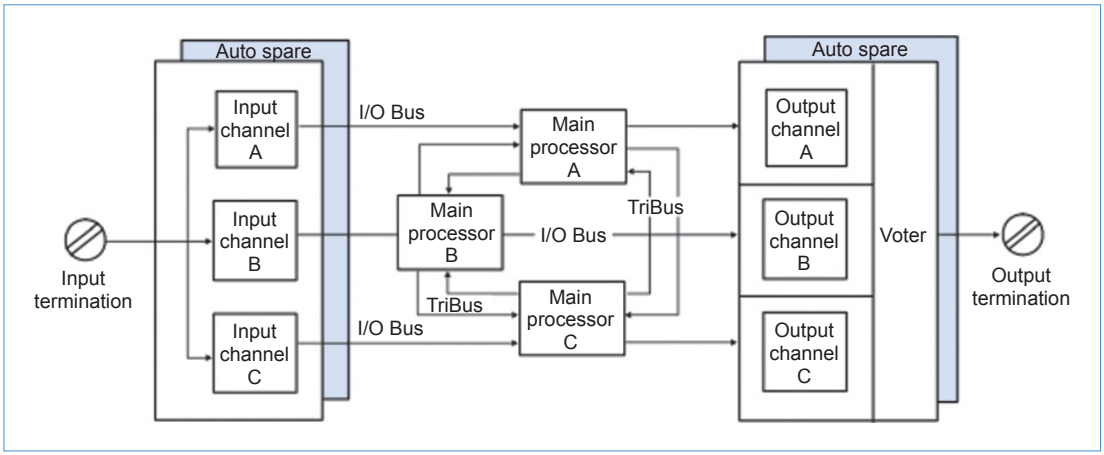

圖 2.
Tricon 控制器架構。

發展之三重容錯控制器 NCS-1000 硬體及軟體設計，第四章說明 NCS-1000 之環境耐受性測試，第五章結論。

二、三重容錯數位控制器硬體設計

1. 三重容錯控制器硬體架構

國際間著名之三重容錯控制器 Tricon 包含三個主處理器 (main processor)，以及具熱插拔之二重化 I/O 模組 (I/O modules)。透過 Tricon 匯流排 (TriBus) 將三個主處理器連接在一起，以硬體脈衝的方式進行同步、輸入投票、邏輯控制、輸出比較以及自我診斷等功能。另外，主處理器與 I/O 模組藉由 I/O 匯流排 (I/O bus) 進行通訊，如圖 2 所示。

同樣地，HFC-6000 控制器也包含三個處理器，透過三重化同步連線 (TMR synchronization link, TSL) 將三個主處理器連接在一起，以權杖傳遞 (token passing) 的方式進行同步、輸入投票、邏輯控制、輸出比較以及自我診斷等功能，如圖 3 所示。另外，主處理器與 I/O 模組的 I/O 匯流排則是採用專用的內部通訊連線 (inter-communication link, ICL) 進行通訊。HFC-6000 控制器在主處理器連接之 TSL 通訊採用二重化的通訊架構，具有更高的可靠性，但設計上也相對複雜許多。

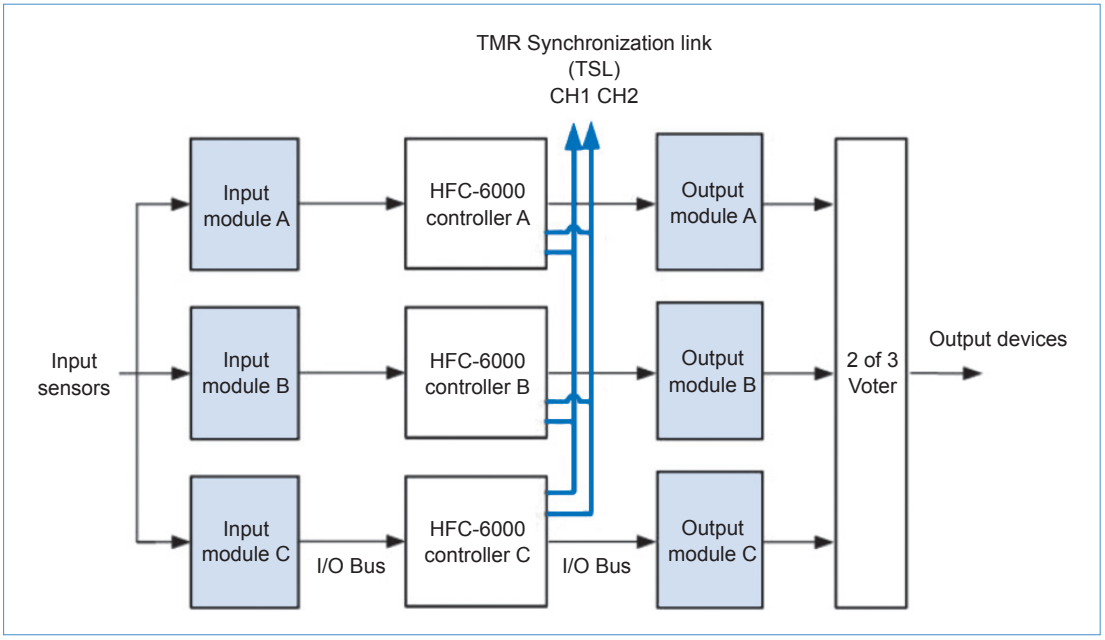

圖 3.
HFC-6000 控制器架構。

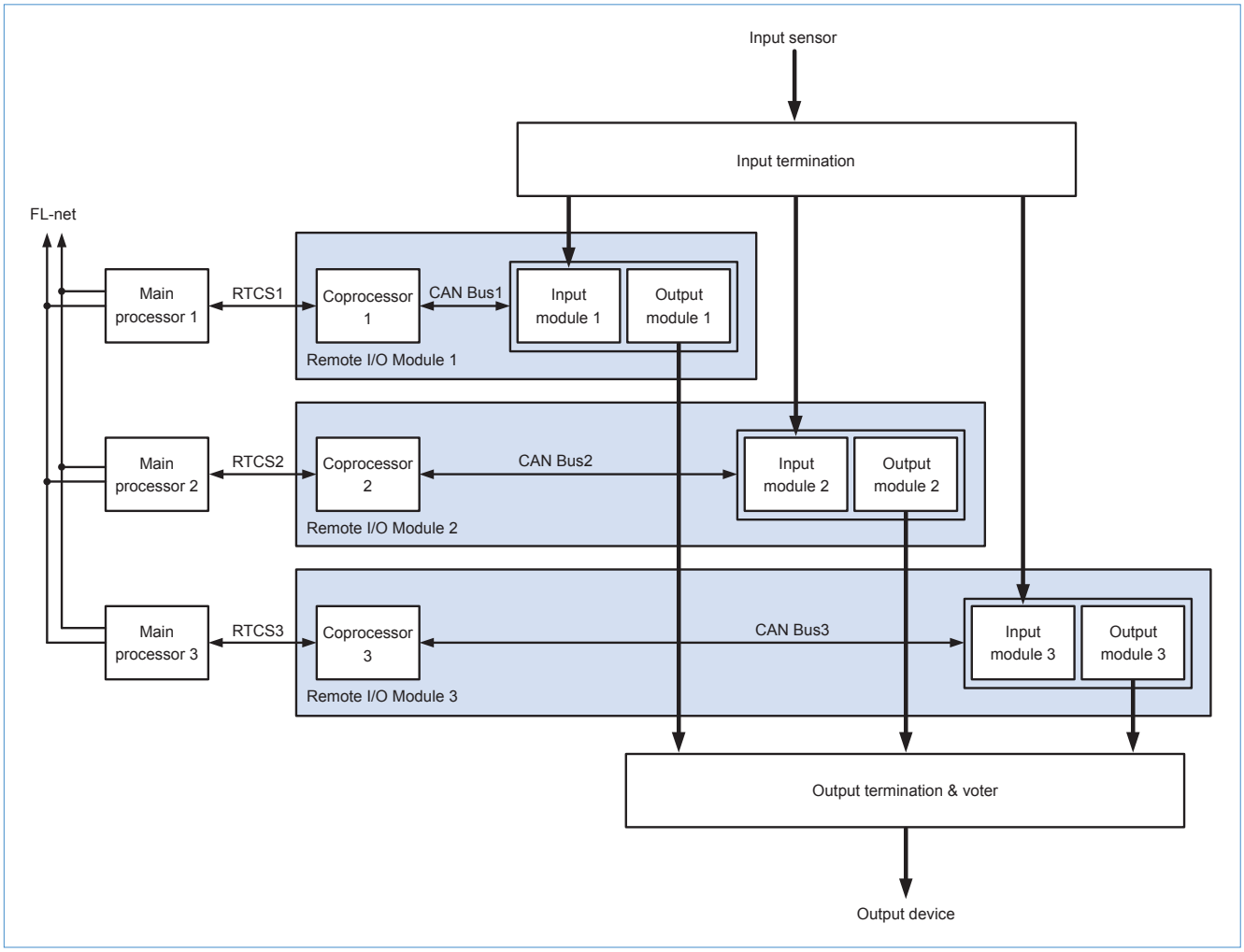

圖 4. NCS-1000 控制器架構圖。

NCS-1000 三重容錯架構如圖 4 所示，包含主處理器、遠端 I/O 模組 (remote I/O modules) 及各式通訊介面等。NCS-1000 主處理器在每次掃描週期內，透過專線與其他相鄰的處理器進行同步與資料交換，並進行輸入訊號的比對，避免進入到主處理器的輸入訊號不一致，主處理器執行完控制程式後會將結果傳送到輸出模組，輸出模組會對輸出訊號進行投票，並檢測與修正主處理器與輸出模組之間發生的錯誤。NCS-1000 各部分說明如下。

(1) 主處理器模組

NCS-1000 的主處理器為一 ×86 架構的工業電腦處理器模組 (processor module)，包括主機板、I/O 埠及對外通訊埠等。處理器模組採用精簡基本輸入輸出系統 (basic input/output system, BIOS) 與即時作業系統 QNX 6.3，配備有記憶體管理單元、內部通訊、自我修復機制以及支援各種周邊設備之驅動程式。

NCS-1000 包含三個主處理器模組，每個主處理器具有一個獨立的訊號通道，並與其他主處理器平行運作。每個輸入模組透過輪詢 (polling) 的方式將新的輸入訊號透過即時用戶與服務端 (real-time client and server, RTCS) 協定傳送到主處理器，與 Tricon 的 I/O 匯流排及 HFC-6000 的 ICL 功能類似。主處理器使用 FL-net 專線對三個主處理器進行同步、資料傳輸以及資料比較等。FL-net 是一種以乙太網路為基礎的 JEMA (Japan Electrical Manufactures Association) 協定標準[5, 6]，具備時間

確定性的特性。同時，FL-net 機制也是一種以權杖傳遞的環狀網路，網路上只有擁有權杖的節點才可以進行廣播，每個節點透過 FL-net 進行廣播，更新共享記憶體。

若輸入訊號發生不一致時，將以投票機制決定最後進入到主處理器控制程式的輸入訊號。同時，每個主處理器透過與其他處理器的資料比較，對自身的記憶體資料進行必要的修正，以確保資料傳輸過程的正確性。主控制器藉由使用者編輯的控制程式產生對應的輸出訊號，並透過 RTCS 傳送到通道上對應的輸出模組輸出。

(2) 遠端 I/O 模組

NCS-1000 採用 RTCS 連結主處理器與遠端 I/O 模組進行資料交換，通道間完全隔離並獨立運作，換言之，單一通道失效不會影響到其他通道失效，而模組之間的共模抑制比 (common-mode rejection ratio, CMRR) 可達 90 dB。在擴充性方面，每個主處理器最大支援 256 個類比輸入／輸出通道，或 1024 個數位輸入／輸出通道，其中類比與數位轉換具 12 位元以上的解析度。此外，I/O 資料交換的反應時間具確定性 (deterministic)，並具備看門狗電路觸發警報與安全失效 (fail-safe) 模式，一旦有故障或不一致的輸出時，將保持在預設之安全狀態。

2. 操作模式 (Operating Mode)

為了確保控制器之設計功能，三重容錯數位控制器定義不同的操作模式，提供使用者在運轉過程中相對應的保護措施。一般而言，三重容錯數位控制器的操作模式可定義如表 2 所列。

NCS-1000 與 Tricon 控制器採上述之操作模式設計；而 HFC-6000 控制器則定義兩種操作模式：(1) 正常操作模式 (normal operating mode)；(2) 測試與診斷模式 (testing and diagnostic mode)。其中正常模式與上述 RUN 模式功能相同，而測試與診斷模式則包括 STOP、PROGRAM 以及 REMOTE 等模式功能。

3. 同步機制 (Synchronization)

同步機制是三重容錯數位控制器中非常重要的設計。三重容錯數位控制器在固定週期時間內，允許每個控制器監視其他通道上的 I/O訊號、執行狀態、時間參數以及診斷資料等。透過互相比較與相對應的失效對策，可維持控制器之設計功能，有效提高系統的可靠度。通常同步機制在開機後初始化與每次掃描週期時執行。Tricon 控制器以硬體脈衝搭配直接記憶體存取 (direct memory access, DMA) 控制器進行同步，實現於控制器背板的 Tricon 匯流排 (TriBus)；而 HFC-6000 控制器則是採用獨立的二重化之乙太網路接口，使用權杖傳遞搭配廣播的方式進行同步。

NCS-1000 採用獨立的乙太網路接口，透過對外通訊之 FL-net 與雙向環形二重化的配置，實現同步機制，如圖 5 所示。在同步 FL-net 網路上，只有主處理器才能進行權杖傳遞並對網路廣播，通訊路由控制器 (communication gateway controller) 只能接收廣播的訊號，並對外通訊，類似防火牆 (firewall) 的保護功能，隔離連外網路對三重容錯數位控制器的影響。

表 2.
NCS-1000 控制器操作模式。

模式	使用時機	說明
RUN	實際運轉	禁止程式寫入與裝置測試，只允許記憶體讀取，確保系統的安全性。
STOP	硬體配置	在所有的程式與控制邏輯進入停機狀態時，允許程式寫入與裝置測試。
PROGRAM	除錯與系統配置	允許程式寫入與裝置測試，所有的程式與控制邏輯可以透過模擬訊號執行測試。
REMOTE	試運轉	禁止程式寫入與讀取，但所有的程式與控制邏輯可以透過模擬訊號執行測試，另外，允許存取記憶體 I/O 區塊操作。

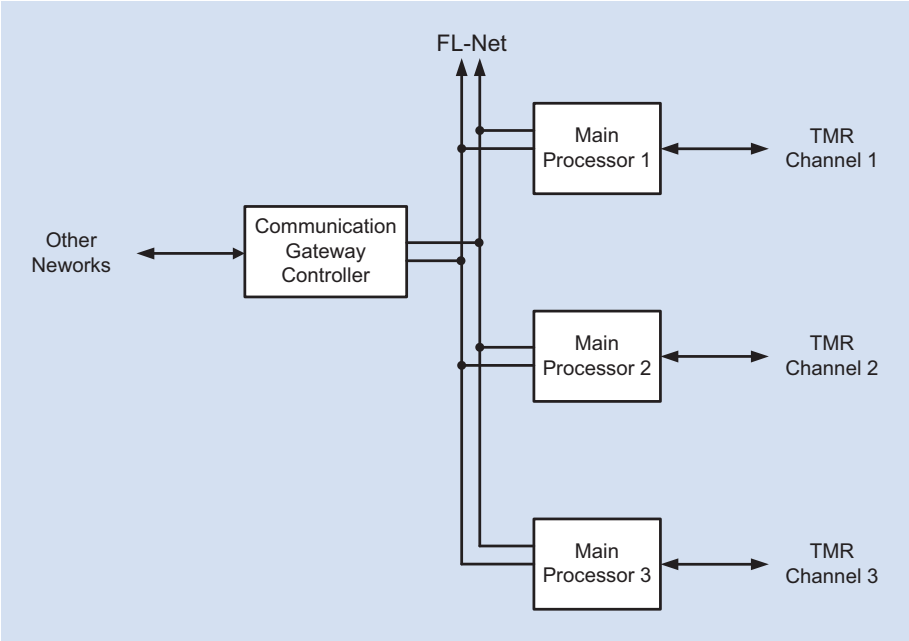

圖 5.
NCS-1000 同步機制設計。

4. 數據通訊 (Data Communication)

由於數位資料在傳輸過程中，因傳輸媒介的可靠度不佳，或外在因素的干擾而遭到破壞[7]，NCS-1000 採用黑色通道 (black channel) 技術來檢測資料傳輸過程中是否遭受到破壞。圖 6 為黑色通道技術示意圖。

黑色通道技術著重於數據通訊的正確性，在訊息資料 (message) 加入下列措施：

(1) 安全碼 (safety code)，如：循環冗餘碼查核 (cyclic redundancy check, CRC)。
(2) 安全程序 (safety procedure)，如：來源識別碼、時間戳記與序列計數等。

透過這些措施，可提升訊息資料在傳輸過程中的可靠性與完整性。相關措施與可檢測到的錯誤關係如表 3 所列。

5. 輸出入模組架構

(1) 輸入模組

NCS-1000 機箱配置三個遠端 I/O 模組，用來處理進入模組的輸入資料，每個通道具有一個微處理器，掃描每個輸入點、編譯資料，並傳送到相應的主處理器。為了確保高度完整性，輸入資料在進入主處理器處理前會先進行投票，NCS-1000 輸入投票機制如表 4 所列，對於輸入模組，所有的關鍵

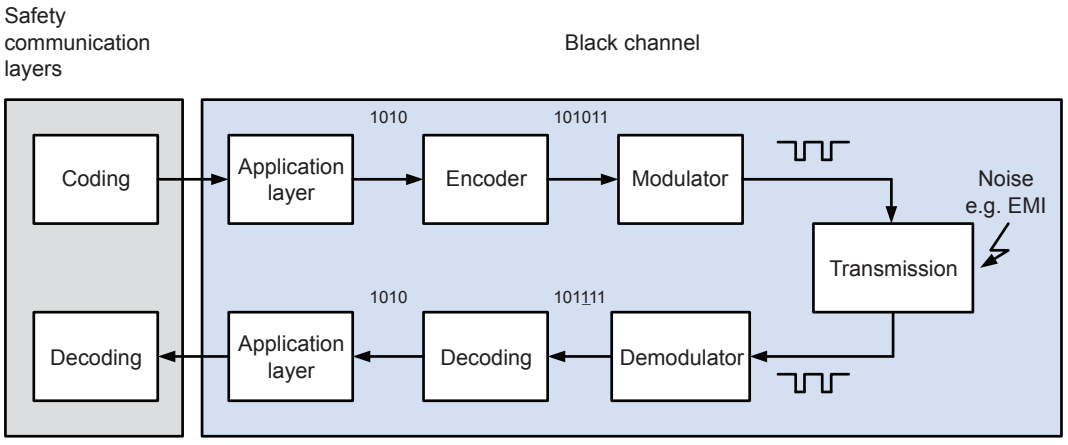

圖 6.
黑色通道技術示意圖。

表 3.
數據通訊相關措施與錯誤檢測。

錯誤 \ 措施	序列編號	看門狗	來源識別碼	CRC
封包重複	■			■
封包遺失	■	■		■
封包插入	■			■
序列編號錯誤	■			■
訊號被破壞				■
過度延遲		■		
假訊號		■		■
交換器內記憶體錯誤	■			■
不正確的轉遞			■	

表 4.
NCS-1000 輸入投票機制。

模式	可用通道數	數位輸出投票	類比輸出投票
三重	3	三選二	中間值
二重	2	二選二	平均值
單一	1	一選一	一選一
安全	0	斷電	NA

訊號路徑皆為三重化，以保證安全與最大可用性。

所有的輸入模組對每個通道持續地進行偵測診斷，任何通道的診斷錯誤將啟動錯誤指示與警報訊號。模組在單一故障時可以保證運轉的正確性，並可以繼續在特定的多重故障模式下正確地運轉。類比輸入模組可透過調整取樣數目，減少異常讀值 (mis-compare readings) 造成的失效；數位輸入模組則利用定值自我測試 (stuck-on or stuck-off test)，週期性地測試光耦合元件是否正常，驗證控制器輸入電路的能力。NCS-1000 之輸入模組電路設計圖如圖 7 所示。

(2) 輸出模組

NCS-1000 在輸出模組方面，與 Tricon 控制器和 HFC-6000 控制器設計近似，每個通道並具有一個微處理器，接收來自相應的主處理器的輸出訊號。NCS-1000 數位輸出模組設計如圖 8 所示，在輸出電路方面，採四重輸出電路 (quadruplicated output circuitry)，比起傳統三選二電路，在關鍵訊號路徑具有最大可用性。圖 9 為 NCS-1000 類比輸出模組設計，在輸出電路方面，採用具週期性之切換電路 (switch circuit)，並透過微處理器與選擇電路 (selector circuit) 隔離異常通道。

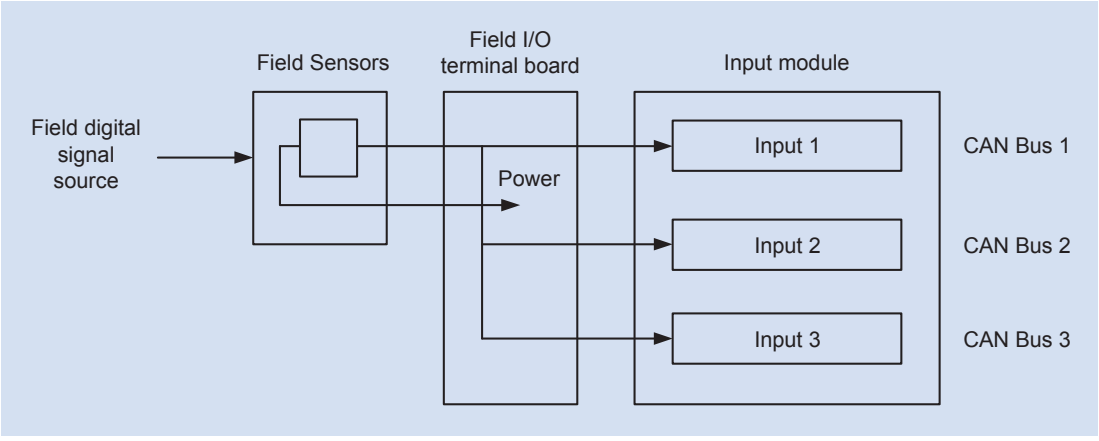

圖 7.
NCS-1000 輸入模組設計。

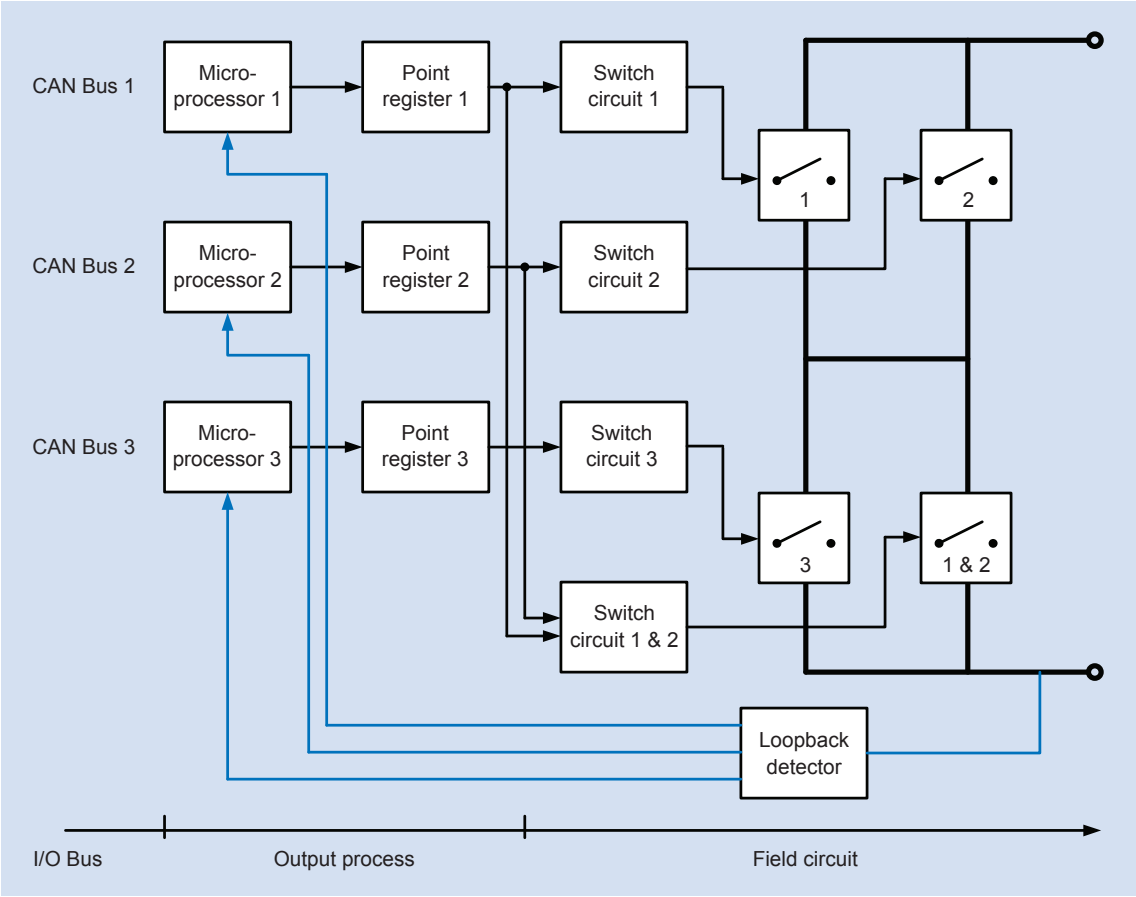

圖 8.
NCS-1000 控制器數位輸出模組設計。

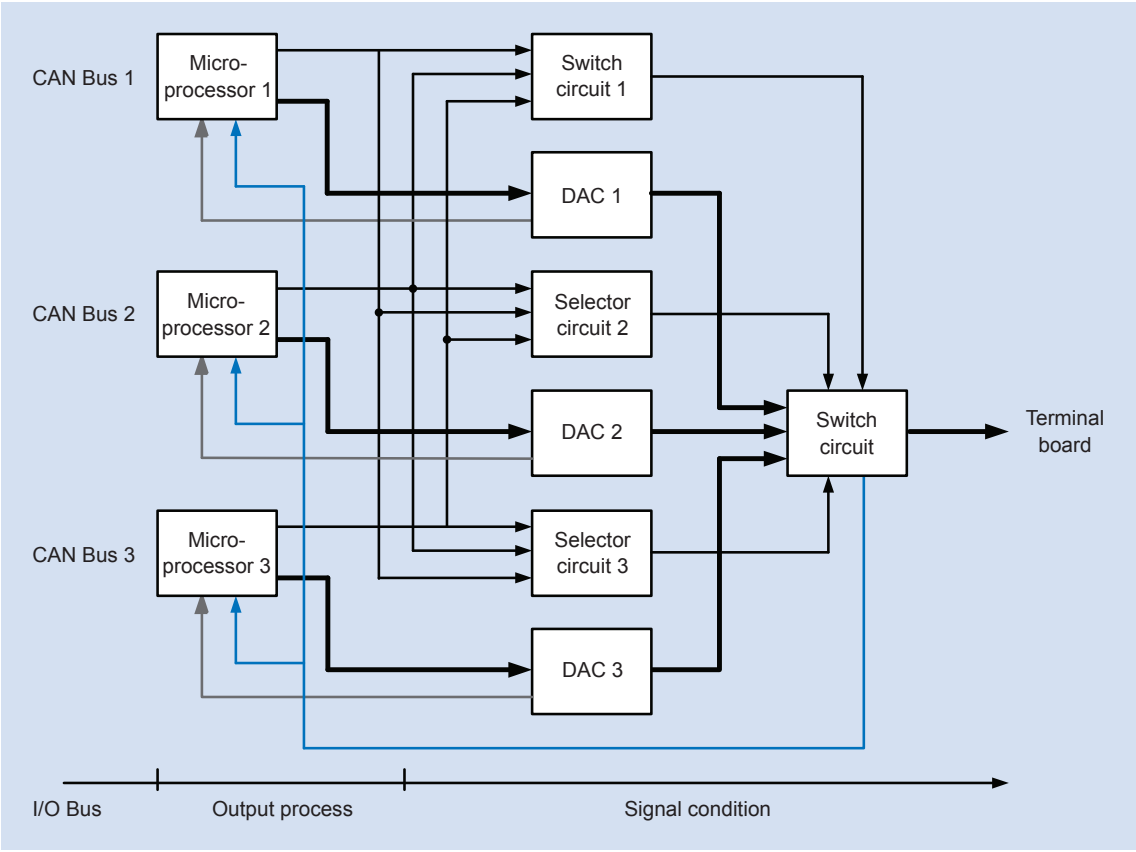

圖 9.
NCS-1000 控制器類比輸出模組設計。

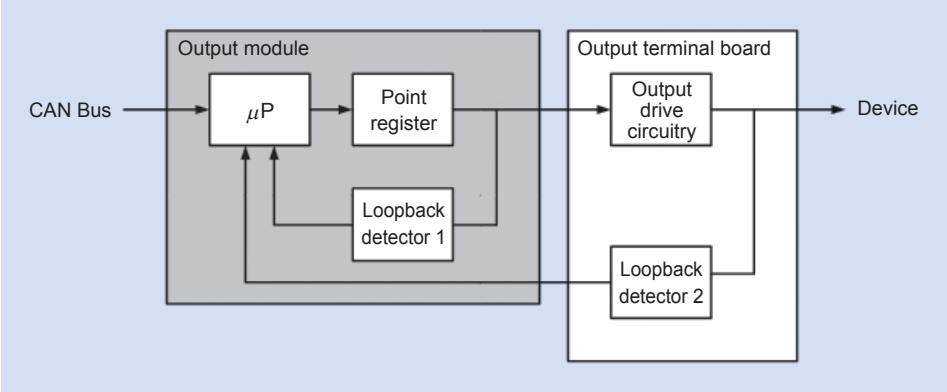

圖 10.
NCS-1000 之環回 (loopback) 測試功能。

NCS-1000 的數位與類比輸出模組以及輸出外接板上，皆具備環回 (loopback) 測試功能，以將訊號送回至傳送端的方式來測試線路是否正常，可有效地進行線上自我診斷並將異常通道隔離，如圖 10 所示。而在數位輸出模組則是對每個輸出點執行輸出投票診斷 (output voter diagnostic, OVD)，利用瞬間反轉的脈波訊號，測試輸出裝置潛在的錯誤。由於 OVD 屬於一種錯誤植入測試 (fault injection test)，所以通常是針對繼電器、螺線管等機電裝置進行測試。

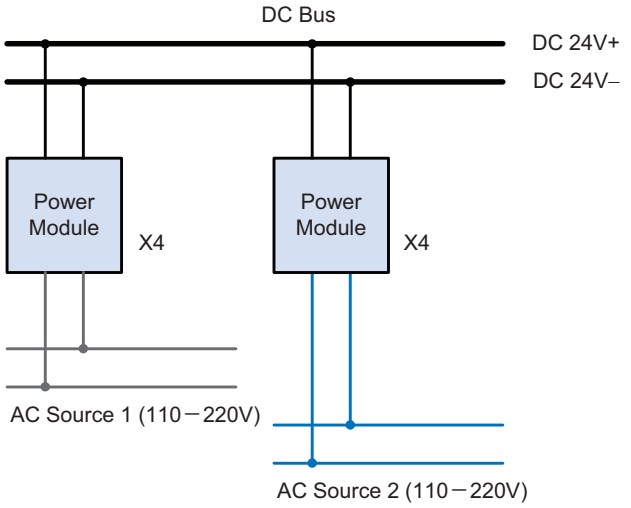

圖 11. NCS-1000 之電源供應器。

Tricon 控制器在數位與類比輸出同樣地採用環回測試設計，而 HFC-6000 控制器在數位輸出採用線圈連續 (coil continuity) 測試設計，較環回測試更為嚴謹。

6. 電源供應器 (Power Supply)

通常三重容錯數位控制器皆具備二重化電源模組，確保單機失效時控制器可維持正常功能運作。NCS-1000 之電源供應器主要提供 DC 24 V 電源，一個電源供應器具有 8 個相同可熱插拔的電源模組，每 4 個電源模組由一個交流電源供電，每個電源模組可提供 150 W 的電源，如圖 11 所示。

NCS-1000 之被動式的負載共享可以確保電源供應器正常供電，以提高可靠度。另外，NCS-1000 之電源供應器還提供了電壓偵測機制，確認電源供應器輸出是否在允許範圍內，如表 5 所列。

三、三重容錯數位控制器軟體設計

1. NCS-1000 軟體架構

NCS-1000 機箱配置三個主處理器，每個主處理器負責一個通道，獨立執行控制程式並與相應的遠端 I/O 模組通訊，不需共用時脈。在固定的週期內，三個主處理器進行資料比較並執行控制程式。

表 5.
電源供應器之電壓偵測機制。

異常狀況	保護模式
外部不當引入電壓高於 DC 24V	過電壓保護 (over voltage protection, OVP)
電源供應器提供之電壓高於 DC 26V	
AC 電源低於 90 V 或 DC 匯流排短路	低電壓保護 (under voltage protection, UVP)
負載超過額定值	過負載保護 (over load protection, OLP)

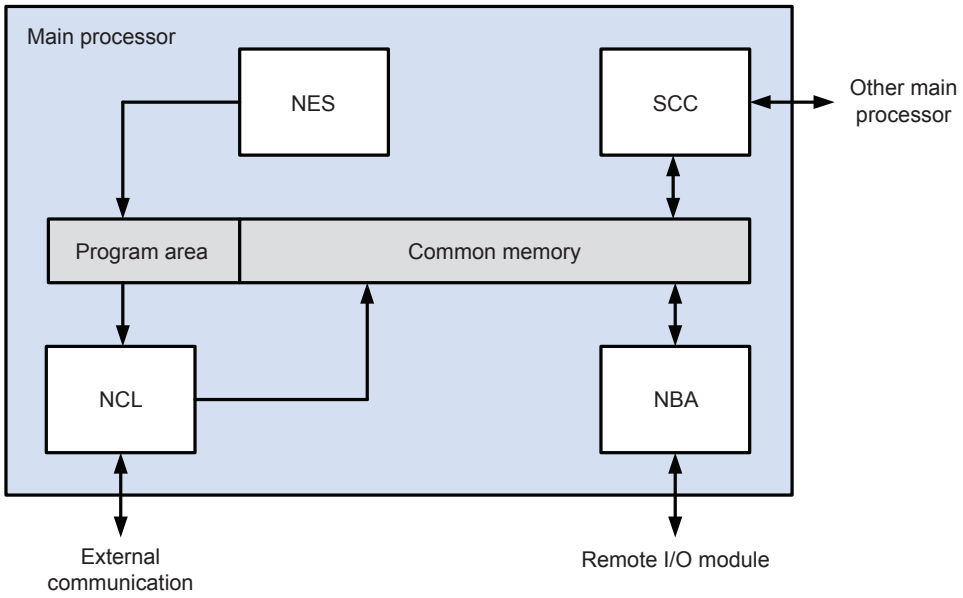

圖 12.
NCS-1000 軟體模組。

每個主處理器內部包括四個主要的軟體模組：新型控制語言 (new control language, NCL)、新型遠端 I/O 匯流排接口 (new remote I/O bus adapter, NBA)、安全交叉比較 (safety cross-compare, SCC)、新型專業服務 (new engineer service, NES)，每個模組透過共享記憶體 (common memory) 進行交換資料，如圖 12 所示。

各軟體模組的說明如下：

(1) 新型控制語言 (NCL)

NCL 為主處理器軟體的核心，主要的功能為執行系統軟體與應用程式。系統軟體為一內置程式，提供系統初始化、I/O 交換、通訊管理、錯誤監測以及錯誤處理等功能；應用程式則是依照使用者的規劃，執行控制系統的輸入與輸出以及控制邏輯運算。應用程式可利用電腦輔助工具，提供圖形化工具編輯，如：階梯圖或功能方塊圖等。同時，電腦輔助工具也可以將圖形化語言轉換為 NCL 的目標代碼，並於 STOP 與 PROGRAM 模式將程式寫入至共用記憶體內。

(2) 新型遠端 I/O 匯流排接口 (NBA)

NBA 主要功能為連接主處理器與遠端 I/O 模組，將來自 I/O 模組的 I/O 資料與共用記憶體內 I/O 資料區的資料進行交換與更新。

(3) 安全交叉比較 (SCC)

由於 NCS-1000 內，控制器之間彼此獨立運作，必須透過 SCC 與其他控制器進行安全交叉比對，達到資料共享與線上自我診斷的目標。未涵蓋於線上自我診斷測試中的錯誤或失效模式 (undetected failures)，必須於週期監視測試 (periodic surveillance testing) 時進行檢測，例如：I/O 資料於每次循環週期進行線上自我診斷，其他安全資訊則於每 8 個小時進行週期監視測試。

SCC 採時間同步 (time synchronization) 機制，使各主處理器的時間 (time clock) 同步，在電源啟動診斷 (power-up diagnostics) 後與 cross-copy 開始時進行同步，如圖 13 所示。同步完成後，開始進行掃描，各主處理器開始交換 I/O 資料、診斷 (diagnostic) 以及通訊資料，比較與前次掃描不一致的輸出訊號，以及應用程式記憶體等。

(4) 新型專業服務 (NES)

NES 透過軟體看門狗來監測其他軟體模組，並且提供在不同模式下資料加載與記憶體讀／寫等功能。由於控制器可能因電源不穩定、電磁波干擾或軟體失效等，進入非預期的閉路循環，看門狗計時器提供故障狀態下之自我恢復的能力。其主要功能為監視主處理器的狀態，在正常狀態下主處理器會定時地更新心跳信號 (heartbeat)，觸發看門

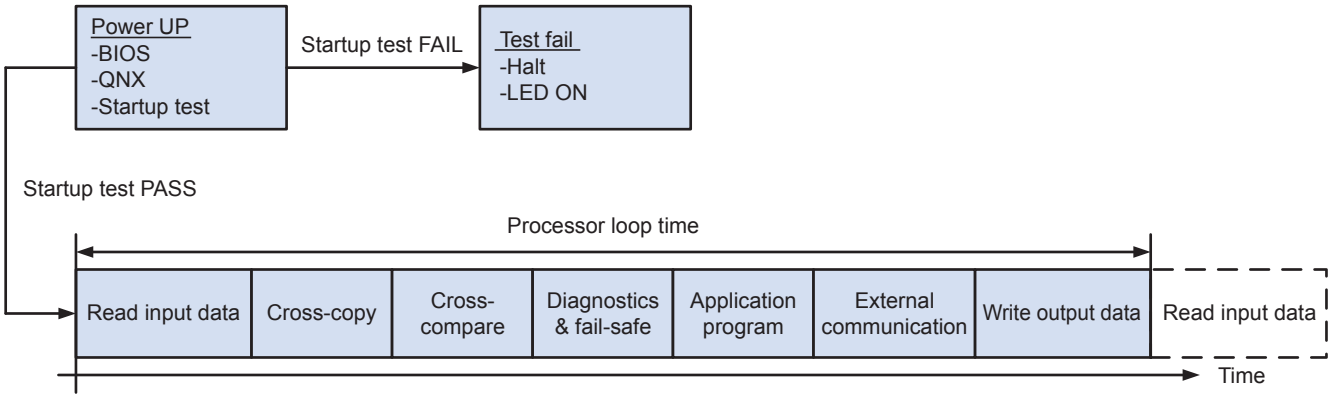

圖 13. NCS-1000 軟體排程。

狗計時器復位；如果控制器發生失效，心跳信號無法在一定的時間觸發看門狗計時器復位，則看門狗計時器的電路將重置該控制器，有效降低檢測和鑑別失效的時間。NES 看門狗計時器設計特性如下：

(a) 當控制器無法即時重置看門狗計時器時，看門狗計時器將設定控制器輸出進入失效安全狀態。
(b) 看門狗計時器與主處理器的時脈訊號相互獨立。
(c) 看門狗計時器為獨立硬體裝置。
(d) 任何通信功能與中斷服務功能皆不能干擾或暫停看門狗定時器的運行。
(e) 當重置狀態被看門狗定計器啟動時，它應該提供警報器功能。
(f) 被動式看門狗計時器設計。

2. 線上診斷與失效對策

為了確保控制器之設計功能，NCS-1000 透過線上診斷軟體不斷地對系統進行故障檢測，以失效或累計錯誤數來判斷錯誤類別，分類如表 6 所示。

當三重容錯數位控制器發生致命錯誤時，為了讓系統復原，控制器必須重新啟動並進行故障排除。當三重容錯數位控制器發生非致命錯誤時，若診斷為單一數位控制器失效，三重容錯數位控制器則以二選二的機制繼續執行控制器功能。而若診斷為單一數位控制器之部分功能失效，三重容錯數位控制器則以三選二的機制繼續執行控制器功能。然而，當上述任一狀況發生時，系統將發出警報訊號並進行適當的因應動作。

表 6.
失效類別與說明。

失效類別	說明	分類	失效對策
致命 (Fatal)	三重容錯數位控制器失效	三重容錯數位控制器之循環 FL-Net 失效 兩台以上的數位控制器失效 兩個以上的跳脫輸出訊號失效 兩個以上的關鍵輸入訊號失效	斷電
非致命 (Non-Fatal)	單一數位控制器失效	一台數位控制器之通訊功能失效 一台數位控制器失效 一個跳脫輸出訊號失效 一個關鍵輸入訊號失效	將失效控制器隔離，並依據表 4 調整系統模式。
	單一數位控制器之部分功能失效	部分周邊、通訊或 I/O 電路失效 FL-Net 通訊錯誤 RTCS 通訊錯誤	維持三選二機制

表 7. NCS-1000 之電磁相容性測試需求。

IEC61000 RG-1.10/RG-1.180/R1 EMI 發射性測試項目				
次	項目	規格範圍		
1	高頻傳導性	IEC61000-6-4, CISPR 11 Class A (150 kHz to 30 MHz) 79 dBμV QP, 66 dBμV AV (150 kHz to 500 MHz) 73 dBμV QP, 60 dBμV AV (500 kHz to 5 MHz) 73 dBμV QP, 60 dBμV AV (5 MHz to 30 MHz)		
2	高頻輻射性	IEC61000-6-4, CISPR 11 Class A (30 MHz to 1 GHz) 30 dBμV QP, at 30 m (30 MHz to 230 MHz) 37 dBμV QP, at 30 m (230 MHz to 1 GHz)		
IEC61000 RG-1.180/R1 EMS 耐受性測試項目				
次	項目	規格範圍	電源線	信號線
1	低頻傳導性	IEC61000-4-13 (16 Hz－2.4 kHz)	✓	
		IEC61000-4-16 (15 Hz－150 kHz)	✓	✓
2	低頻傳導性	IEC61000-4-6 140 dBμV (150 kHz to 80 MHz)	✓	✓
3	低頻輻射性	IEC61000-4-8 (50 & 60 Hz)		
4	高頻輻射性	IEC61000-4-9 (50 Hz to 50 kHz) IEC61000-4-10 (100 kHz to 1 MHz) IEC61000-4-3 140 dBμV/m (26 MHz to 1 GHz)		
5	電氣快速暫態 (EFT)	IEC61000-4-4 ± 4 kV (Power line), ± 2 kV (Signal line)	✓	✓
6	雷擊突波 (SURGE)	IEC61000-4-5 ± 4 kV (Power line), ± 2 kV (Signal line)	✓	✓
		IEC61000-4-12 (Ring wave) ± 4 kV (Power line), ± 2 kV (Signal line)	✓	✓
7	靜電放電 (ESD)	IEC61000-4-2 ± 8 kV (Contact), ± 15 kV (Air)		

四、環境耐受性測試

為驗證控制器在不同操作環境下之可靠度，NCS-1000 已進行不同的環境驗證測試，符合下列標準要求：

(1) 耐溫度及溼度測試符合 IEEE 381-1977[8] 之要求。
(2) 耐震測試符合 IEEE 344[9] 之要求。
(3) 耐輻射測試符合累積劑量達到 1000 rads 之要求。
(4) 元件老化分析符合 IEEE 323-1983[10] 之要求。
(5) 耐電磁波能力測試符合 IEC-61000[11] 之要求。
(6) 耐震測試符合國內台電公司核一、二、三、四廠之地震需求反應頻譜。

其中，耐電磁波能力必須通過：(1) 可承受外界干擾之電磁耐受性 (electro-magnetic susceptibility, EMS)，以及 (2) 本身產生干擾之電磁干擾性 (electro-magnetic interference, EMI) 兩項測試。表 7 說明 NCS-1000 之電磁相容性測試標準要求。

另外，耐震測試通過台電公司核一、二、三、四廠運轉基準地震 (operating basis earthquake, OBE) 與安全停機地震 (safe shutdown earthquake, SSE) 之需求反應頻譜 (required response spectra, RRS)，如圖 14 所示。

五、結論

本文介紹台灣本土化自主型儀控技術之建立，透過整合國內已發展成熟的工業級控制系統，發展具高可靠度之三重容錯控制器，也介紹在國內進行之環境耐受性測試，期望能應用於國內需求高可靠度的系統上。

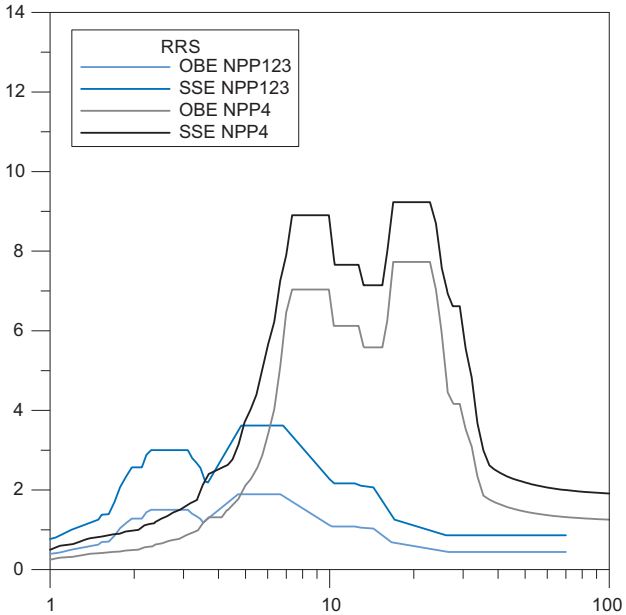

圖 14. 台電核一廠至核四廠的地震需求反應頻譜。

參考文獻

1. P. B. Ladkin, IEC 61508, International Electrotechnical Commission (2010).
2. NRC, Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report (2001).
3. A. Hsu, *HFC-6000 Safety Control System Safety concept, RR901-000-22*, Rev. D, Doosan HF Controls Corporation (2009).
4. S. F. Hsieh, T. H. Wu, and Y. K. Su, *Digital Controller Design and Application in Taiwan*, International Workshop on the Establishment of TaiNICS (2009).
5. JIS B 3521, Protocol specification for FA control network standard, Japanese Industrial Standards (2004).
6. JEM TR-214, Device profile common specification for FA control network, Japan Electrical Manufactures Association (2000).
7. S. Brown, *Computing & Control Engineering Journal*, **11**, 6 (2000).
8. IEEE 381, IEEE standard criteria for type tests of class 1E modules used in nuclear power generating stations, Institute of Electrical and Electronics Engineers (1977).
9. IEEE 344, IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers (1987).
10. IEEE 323, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers (1983).
11. IEC 61000, Electromagnetic compatibility (EMC), Geneva, Switzerland (2006).

徐獻星先生為美國賓州州立大學核工博士，現任核能研究所核能儀器組研究員。

Shian-Shing Shyu received his Ph.D. in nuclear engineering from Pennsylvania State University, U.S.A. He is currently a researcher at Nuclear Instrumentation Division, Institute of Nuclear Energy Research.

陳昌國先生為國立成功大學工程科學博士，現任核能研究所核能儀器組副研發師。

Chang-Kuo Chen received his Ph.D. in engineering science from National Cheng Kung University. He is currently an assistant developer at Nuclear Instrumentation Division, Institute of Nuclear Energy Research.