Holtek MCU UL / IEC 60730 認證對策

文件編碼：AN0584TC

簡介

國際電工委員會(IEC)制定了家電開發的安全標準 IEC 60730。

IEC 60730-1 標準(家用和類似用途的自動電氣控制器－第 1 部分：通用要求)規定了測試和診斷方法，以確保家電中受控設備的安全操作。按此標準，家用電器的設計者應確保產品在正常使用中，或在使用者有粗心大意、錯誤操作的情況下，也不會對人員及周圍財產造成損害。附錄 H 是該標準的關鍵部分，將軟體分爲 Class A、Class B、Class C 三個等級，家電製造商必須按照這三個等級的規則設計他們的產品。

本文根據相關標準，考量晶片實際情況，推薦利於用戶通過 IEC 60730 認證的一些對策，同時解釋 IEC 60730 對應的條款、測試的內容，幫助用戶更清晰地瞭解 IEC 60730 各個測試項目的測試要求，有針對性地開發自檢程式，加速認證過程。

功能說明

IEC 60730 標準規定了家用電器的三種等級，三種等級的差異如下所述。

Class A：電器安全不依靠軟體，或電器不會造成人員傷害，如 LED 照明產品，不需要軟體認證，本文不做說明。

Class B：防止家電因不安全的操作造成傷害，如洗衣機的電控門鎖、電機熱關斷機制等。

Class C：防止發生特殊的危害，如電子點火燃氣灶(有爆炸危險)。

Class B 測試總表

代號	組件/功能	故障/錯誤	認證對策	對策定義
1.1	CPU/暫存器	阻塞故障	靜態記憶體的週期自檢測試(用數據 0x55、0xAA 檢查每個 CPU 暫存器)	H.2.19.6
1.3 2 3 6.3	CPU/程式計數器 中斷處理和執行 時鐘 外部通訊/計時	阻塞故障 無中斷或過於頻繁的中斷 錯誤頻率 時間點/順序錯誤	獨立的時隙和邏輯監測	H.2.18.10.3
4.1 4.3 5.1 5.2	不變記憶體 不變記憶體的尋址 到不變記憶體的數據路徑 不變記憶體的尋址	所有單 bit 錯誤 阻塞故障 阻塞故障 錯誤地址	校驗和的週期自檢 或 CRC-16 的週期自檢	H.2.19.3.1 H.2.19.4.2

代號	組件/功能	故障/錯誤	認證對策	對策定義
4.2 4.3 5.1 5.2	可變記憶體 可變記憶體的尋址 到可變記憶體的數據路徑 可變記憶體的尋址	DC 故障 阻塞故障 阻塞故障 錯誤地址	靜態記憶體的週期自檢測試(March C-演算法或 March X 演算法)	H.2.19.6
6.1 6.2	外部通訊/數據 外部通訊/尋址	漢明距離≥3 錯誤地址	含數據、地址的冗餘傳輸(正碼與反碼)	H.2.18.2.2
7.1 7.2.1 7.2.2 5.1 5.2	數字 I/O 模擬 I/O(A/D 和 D/A) 模擬多路複用器 到 I/O 組件的數據路徑 I/O 組件的尋址	H.27 中規定的故障狀態 H.27 中規定的故障狀態 尋址錯誤 阻塞故障 錯誤地址	可信性檢查	H.2.18.13
	看門狗(獨立時鐘源)	太快/太慢/時鐘卡滯	超時後重置 CPU(上電測試一次)	

Class C 測試總表

代號	組件/功能	故障/錯誤	認證對策	對策定義
1.1	CPU 暫存器	DC 故障	記憶體的踱步式週期自檢測試	H.2.19.7
1.2	CPU 指令解碼和執行	解碼或執行錯誤	等價性等級測試的週期自檢測試	H.2.18.5
1.3 2 3	CPU 程式計數器 中斷處理和執行 時鐘	DC 故障 無中斷或過於頻繁的中斷 錯誤頻率	獨立時隙和邏輯監測	H.2.18.10.3
1.4 1.5	CPU 尋址 數據路徑的指令解碼	DC 故障 DC 故障和執行錯誤	由 1.2、4.3、5.1、5.2 覆蓋	
4.1 4.3 5.1 5.2	不變記憶體 不變記憶體的尋址 到不變記憶體的數據路徑 不變記憶體的尋址	所有資訊錯誤的 99.6%覆蓋率 DC 故障 DC 故障 錯誤地址和多次尋址	CRC-16 的週期自檢	H.2.19.4.2
4.2 4.3 5.1 5.2	可變記憶體 可變記憶體的尋址 到可變記憶體的數據路徑 可變記憶體的尋址	DC 故障和動態耦合 DC 故障 DC 故障 錯誤地址和多次尋址	記憶體的踱步式週期自檢測試	H.2.19.7
6.1 6.2	外部通訊/數據 外部通訊/尋址	漢明距離≥4 錯誤和多重尋址	含數據、地址的 CRC-16 檢驗	H.2.19.4.2
6.3	外部通訊/計時	時間點/順序錯誤	時隙監測	H.2.18.10.4
7.1 7.2.1 7.2.2 5.1 5.2	數字 I/O 模擬 I/O(A/D 和 D/A) 模擬多路複用器 到 I/O 組件的數據路徑 I/O 組件的尋址	H.27 中規定的故障狀態 H.27 中規定的故障狀態 尋址錯誤 DC 故障 錯誤地址和多次尋址	輸入、輸出的測試模式	H.2.18.22
	看門狗(獨立時鐘源)	太快/太慢/時鐘卡滯	超時後重置 CPU(上電測試一次)	

IEC 60730 規定中涉及的兩種常見故障類型說明如下。

阻塞故障(Stuck-at Fault)，由於出現雜質、CMOS 柵氧斷裂、靜電損壞等，儲存單元或信號線間斷路或短路(Stuck Open / Stuck at 1/ Stuck at 0)。

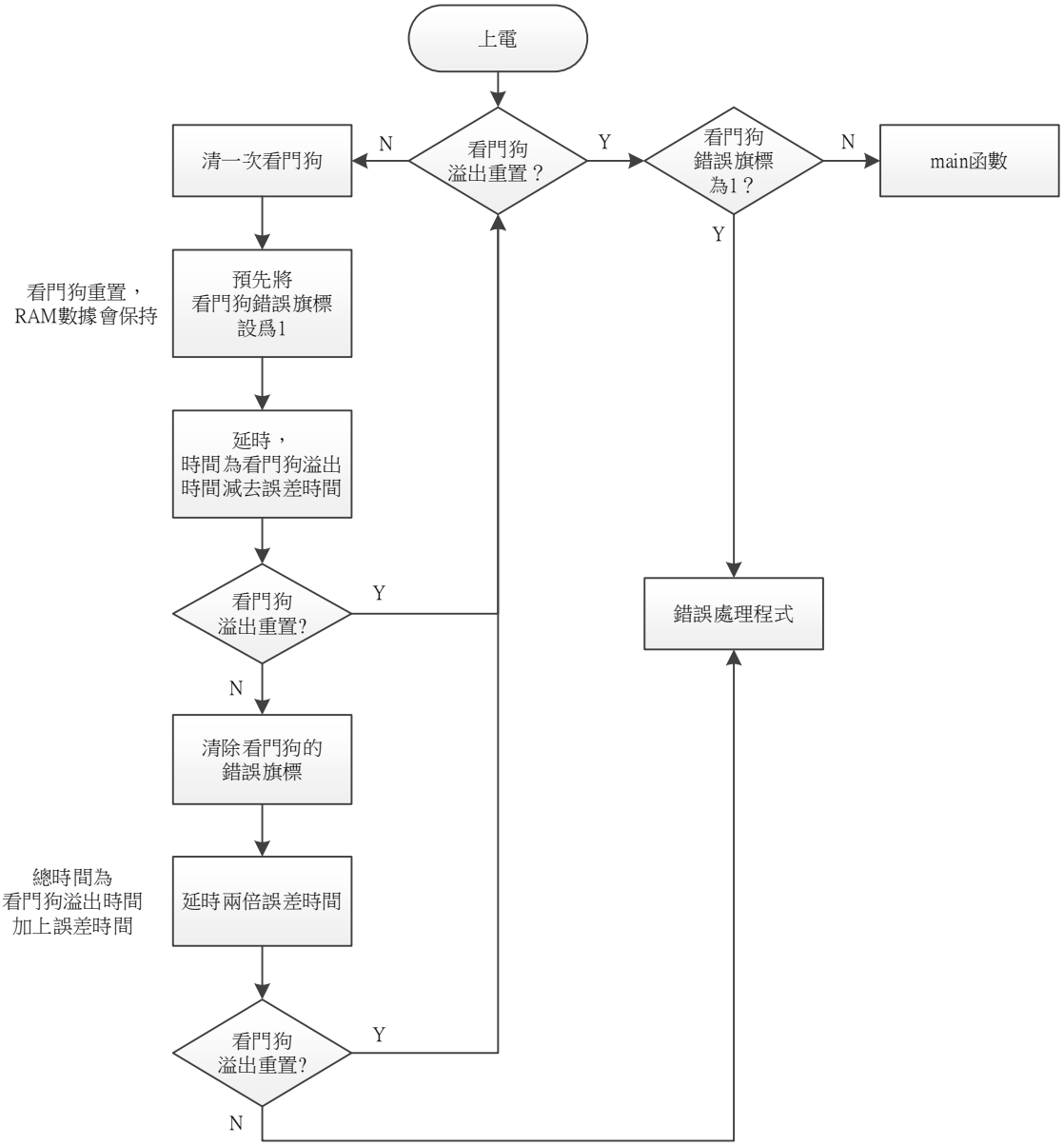
DC 故障(DC Fault)，包含阻塞故障、橋接故障等儲存單元、信號線間多種故障模型。

Class B 認證對策

看門狗

測試定義：儘管在 IEC 60730 中沒有規定，但是對於跟 MCU 集成在同一片晶圓上的看門狗，通常會要求測試其是否正常工作，避免出現重置時間太快、太慢或卡滯不工作的情況。同時要求使用有別於系統時鐘的獨立時鐘源(如 32kHz 的 LIRC 或 32768Hz 晶振)，以確保在必要時能正確地將 MCU 與輸入/輸出端口非同步重置為已知安全狀態。

認證對策：在 MCU 上電後，運行其他代碼前測試一次。需考慮系統頻率的誤差及不同電壓、溫度下的頻率漂移，故可接受的誤差時間範圍應適當擴大。如下流程可供參考。



CPU 暫存器

測試定義：靜態記憶體測試(Static Memory Test)，一種僅用於檢測靜態錯誤的故障/錯誤控制技術。

認證對策：從 ACC 暫存器開始，用 0x55、0xAA(部分認證機構可能要求額外增加 0x00、0xFF 數據)分別填充全部 CPU 暫存器(可能引起 CPU 工作異常的特殊暫存器除外)，再讀出對比，測試是否正常。

CPU 程式計數器、中斷處理和執行、時鐘、外部通訊的計時

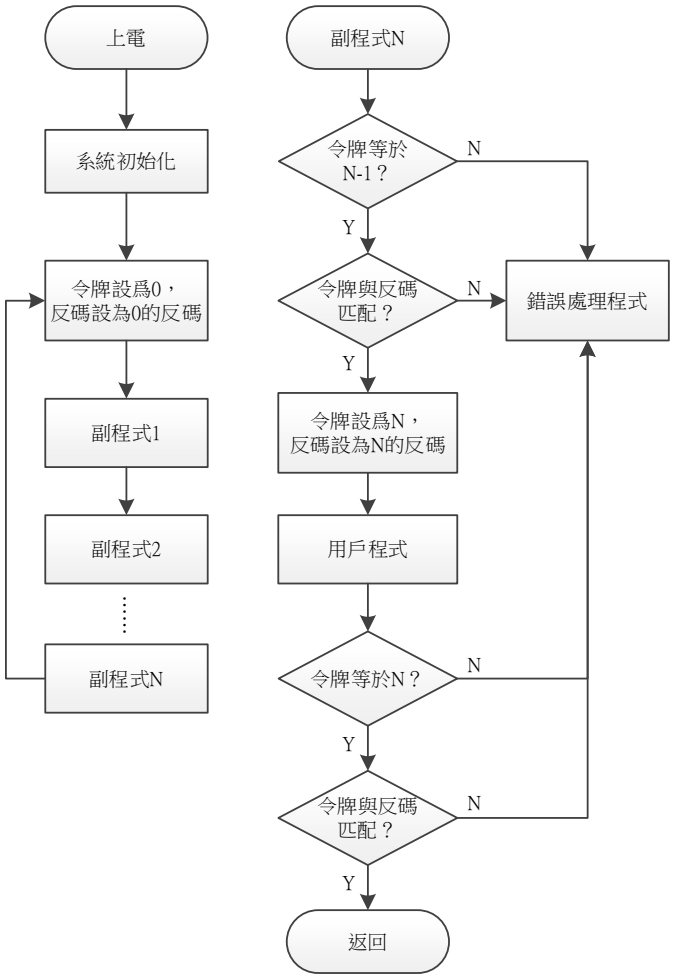
測試定義：獨立的時隙和邏輯監測(Time-slot and Logical Monitoring)，週期地觸發基於獨立時鐘基準的計時裝置而用於監測程式功能和順序的一種故障/錯誤控制技術。

認證對策：令牌傳遞法。

CPU 程式計數器

可定義唯一的一個令牌變量，而每個副程式有自己獨一的令牌號碼，令牌在副程式間傳遞、對比，以確認程式按順序執行。因記憶體自身可能出現故障，故需設定令牌的反碼，校驗令牌自身正確性。

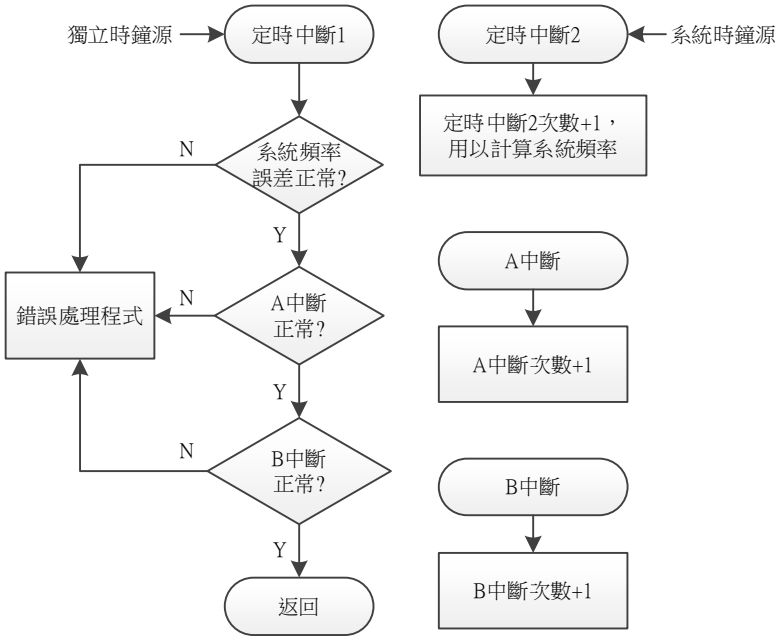
更進一步的，可以先確定副程式的實際運行時間，然後在一個固定時間的中斷內週期性查詢令牌，並與上一次的值做比較，檢驗程式是否在某個副程式停留時間過長。



中斷、系統時鐘

因為中斷的發生有隨機性，監測較為困難，需在每個中斷定義自己的令牌，用於記錄進入當前中斷的次數，然後在一個獨立時鐘的週期性中斷內檢查其他中斷的發生次數，以判別是否有頻繁中斷或無中斷的故障。

監測系統時鐘時，需有兩個定時中斷，一個使用系統時鐘，一個使用獨立時鐘，兩個定時中斷交叉驗證中斷次數，檢測系統時鐘頻率是否超出規格。



不變記憶體

測試定義：校驗和監測(Modified Checksum)，產生並儲存代表記憶體中全部字內容的一個單字的一種故障/錯誤控制技術。在自檢期間，從相同的演算法中生成一個校驗和，並與被儲存的校驗和做比較。該技術能識別所有奇數錯誤和部份偶數錯誤。

雙字的循環冗餘檢查(CRC-double Word)。產生代表記憶體內容的至少二個字的一種故障/錯誤控制技術。在自檢期間，使用相同的演算法產生相同數量的特徵字與儲存的字做比較。不變記憶體的 CRC-16 演算法可確保沒有單 bit 錯誤。

認證對策：HT8 推薦檢查校驗和，HT32 推薦用 CRC16，校驗和/CRC 簽名預先儲存在 EEPROM 或 Flash 中。

對於 HT8，Flash 為高低兩個位元組，編譯器生成的校驗和對應也是兩個位元組。計算方法是：

CheckSum16 = CheckSum16 + FlashHighByte + FlashLowByte

CheckSum16 初值為 0x0000，計算結果如正確，應與編譯器給出的[Program Checksum]一致。

對於 HT32，推薦用 CRC16-CCITT，多項式為 $x^{16}+x^{12}+x^5+1$。建議一個 CRC 簽名用於檢測 32KB 的 Flash，可以更可靠地檢測單 bit 故障。如果 Flash 大於 32KB，可以設置多個 CRC 簽名。如果 Flash 大於 64KB，則推薦選用硬體 CRC，軟體計算會花費較多的計算時間。

CRC 的軟體計算有三種方法。

1. 按 bit 計算：即先將數據的第一個位與多項式進行模二除法，得到一個餘數，再將餘數右移一位加上(不進位加法)第二個位再與多項式進行模二除法，循環計算到最後一位。此方法佔用空間小，但運算量大，不推薦使用。
2. 按 8-bit 計算：即事先計算出 0x00~0xFF 共 256 個 16-bit 的 CRC 碼，存放在 Flash 中，程式直接呼叫，做位元組與位元組的計算。此法佔用空間大，但運算量小，推薦此種方法。
3. 按 4-bit 計算：只需儲存 0x0~0xF 共 16 個 CRC 多項式碼，佔用空間只有按位元組計算的 1/16，計算量大約多 1 倍，屬計算量與佔用空間各有妥協的折中方法。

可變記憶體

測試定義：行進式記憶體測試(Marching Memory Test)，一種靜態記憶體測試，如正常操作一樣，把數據寫入到待測記憶體區域內，按地址昇冪測試每個單元，並對內容執行位元取反。然後按地址降冪重複測試和位元取反。

認證對策：透明的 March C-或 March X 演算法，以及全局變量的動態冗餘校驗。

可變記憶體大致可簡化為以下幾個功能模組：記憶體矩陣、行地址譯碼器、列地址譯碼器、多路轉換器、讀/寫驅動電路。

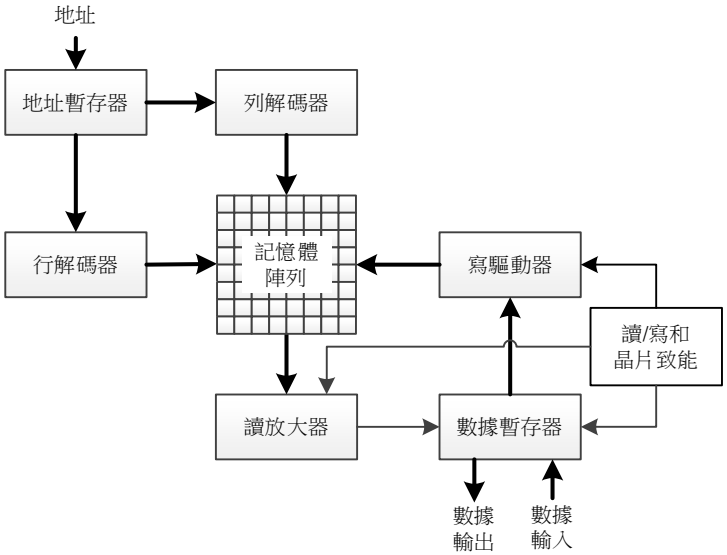


圖 1. 可變記憶體功能模組

記憶體有複雜的結構，對應也存在複雜的故障類型，如下表格所示。

故障類型		故障描述
阻塞故障	SAF Stuck At Fault	儲存單元或信號線被固定地阻塞在某一邏輯值(恆為 0 或恆為 1)。阻塞故障是目前記憶體製造中普遍存在的故障。
轉換故障	TF Transition Fault	儲存單元不能從 0 變為 1，或者不能從 1 變為 0。
耦合故障	CF Coupling Fault	改變單元 i 的數據引起單元 j 的數據跳變。兩相鄰單元的耦合問題可分為： ● 反向耦合(CFin, inversion)：讀/寫儲存單元 i 引起單元 j 的值變反 ● 等冪耦合(CFid, idempotent)：讀/寫儲存單元 i 引起單元 j 的值固定在 0 或 1 ● 狀態耦合(CFst, state)：儲存單元 i 給定 0 或 1，單元 j 出現讀/寫錯誤
橋接故障	BF Bridging Fault	相鄰儲存單元因為橋接而產生的故障。
保持故障	RF Retention Fault	儲存單元經過一段時間 T 後無法維持自己的初始邏輯值。
地址譯碼故障*	AF Address decoder Fault	有四種情況：1 個地址不能訪問任何儲存單元、1 個地址可以訪問多個儲存單元、1 個儲存單元無法被任何地址訪問、1 個儲存單元可以被多個地址訪問。
讀/寫電路故障*		一般表現為阻塞故障或橋接故障。

*備註：地址譯碼故障與讀寫電路的故障，可模型化映射為儲存單元的故障，不單獨檢測。

針對記憶體的故障，有多種演算法做測試，March 演算法是常用的一種，其基本原理是利用有限狀態機，對所有的 bit 逐個進行讀寫操作。演算法的指令比較簡單，只有讀寫 0/1 和地址變化，通過對記憶體不斷地讀寫，能夠檢測幾乎所有的記憶體故障。

為了提高測試效率，在 March 演算法基礎上，採用不同的測試步驟，衍生出 MATS、March C+、March C、March C-、March X 等許多變形。

按程式複雜度與故障覆蓋率，推薦 March C-、March X 演算法，演算法步驟如下。

演算法	覆蓋故障範圍	演算法步驟
March C-	SAF、AF、TF、CF	(w0)；↑(r0,w1)；↑(r1,w0)；↓(r0,w1)；↓(r1,w0)；(r0)
March X	SAF、AF、TF、CFin	↑(w0)；↑(r0,w1)；↓(r1,w0)；↓(r0)

在上述演算法步驟中，各個符號的意義如下。

符號	意義
↑	地址昇冪，由地址 0 遞增到地址 n-1
↓	地址降冪，由地址 n-1 遞減到地址 0
無箭頭	任選地址昇冪或降冪
( )	單個測試步驟，按內部從左到右順序，對單個儲存單元執行讀/寫操作
w0、w1	單個儲存單元寫 0、寫 1
r0、r1	讀單個儲存單元，判斷是否為 0、為 1

舉個例子，↑(r0,w1)，代表從地址 0 開始，先讀出數據判斷是否為 0，接著寫入數據 1；地址遞增 1，對地址 1 做讀、寫動作；一直重複，直到全部地址操作完成。

在傳統的 March 演算法中，測試數據均是按 bit 操作。

由於可變記憶體 RAM 是按 byte 排列的，為提高測試效率和故障覆蓋率，需要擴展測試數據，擴展後的數據稱為數據背景，此時，w1 代表寫入正向數據背景，w0 代表寫入反向數據背景。

8 位數據背景。

正向數據背景	反向數據背景
00000000	11111111
01010101	10101010
00110011	11001100
00001111	11110000

32 位數據背景。

正向數據背景	反向數據背景
00000000000000000000000000000000	11111111111111111111111111111111
01010101010101010101010101010101	10101010101010101010101010101010
00110011001100110011001100110011	11001100110011001100110011001100
00001111000011110000111100001111	11110000111100001111000011110000
00000000111111110000000011111111	11111111000000001111111100000000
00000000000000001111111111111111	11111111111111110000000000000000

不管是 March C-還是 March X 測試，都會覆寫 RAM，破壞原有數據，而 IEC 60730 標準要求做週期性檢測，不只是上電測一次，因此需要使用一些手段，不破壞原有的 RAM 數據，我們稱此為透明測試。

透明測試需要先將 RAM 分區。假設 RAM 劃分為三個區域：RAM1、RAM2、RAM3，RAM3 為測試備份區，僅用於在測試過程備份其他 RAM 分區的數據。測試時先在 RAM3 做 March 測試，再依次將 RAM1、RAM2 的數據備份到 RAM3，再做 March 測試，完成後恢復數據。測試開始前需要先關閉中斷，以免中斷的數據異常。

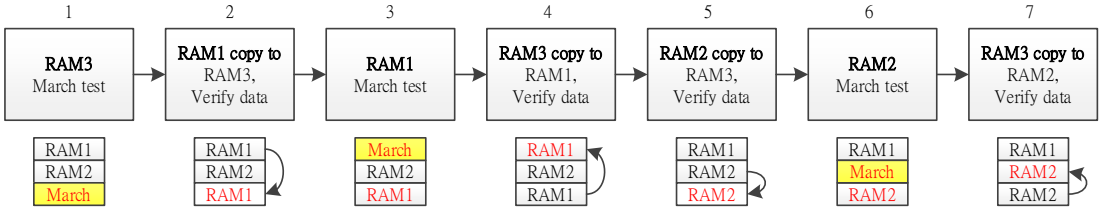


圖 2. 透明的 March 測試

March 測試需要較長時間，可將整個測試切分為多個測試片段，每次僅測試一個 RAM 片段，避免連續長時間佔用 MCU 資源。

以上測試僅可檢測出記憶體的靜態錯誤，如果記憶體發生動態錯誤(即記憶體保存的數據被改變，但未造成記憶體物理性的損壞)，例如外界輻射干擾使得記憶體中某個數據發生跳變，就需要用動態冗餘校驗，保證數據可靠性。

全局變量的動態冗餘校驗，指將全局變量(尤其是與安全相關的變量)以反碼的格式保存在記憶體物理分區的冗餘儲存區域。

用戶需自行將完整的記憶體劃分為至少三個區域。

區域 1：臨時變量區，或編譯器使用
區域 2：全局變量存儲區
區域 3：全局變量冗餘區

保存數據時，先將數據存入區域 2，再在區域 3 的對應位置保存數據的反碼。讀出數據時，同時讀出區域 2、區域 3 對應位置的數據，判斷是否互為反碼，正確則繼續操作，不正確則進入錯誤處理程式。

外部通訊

測試定義：傳輸冗餘(Transfer Redundancy)，數據被至少連續傳輸二次，然後進行比較的一種代碼安全形式。這種技術可識別偶然性錯誤。

漢明距離(Hamming Distance)，體現代碼發現和糾正錯誤的能力的一種統計度量方法。漢明距離等於兩個等長字串對應位置的不同數據的個數，如 1011101 與 1001001 的漢明距離是 2。

認證對策：發送方先傳輸一次地址與數據，緊接著傳輸一次對應的反碼，接收方收到數據後，對比兩筆數據一致性，可判斷數據傳輸是否出錯。

另外，也可選擇在一筆數據的末尾加上校驗和或 CRC 簽名，則可以用一筆數據判別是否發生傳輸錯誤。

I/O

測試定義：可信性檢查(Plausibility Check)，對輸入和輸出進行檢查，以確認是否存在不可接受的數據的一種故障/錯誤控制技術。

測試模式(Testing Pattern)，用於週期性地測試控制器的輸入裝置、輸出裝置和介面的一種故障/錯誤控制技術。將測試模式引入單元並將結果與期望值比較。使用相互獨立的測試模式引入和結果評價。試驗模式的建立應不至於影響控制器的正常操作。

認證對策：使用合理性檢查，檢測指定的故障狀態。

對於數字 I/O，選用恰當的 I/O，輸出 0/1，再檢查 I/O 狀態是否正常，以及 I/O 與電源之間是否有短路或開路。對可能會導致危險的關鍵信號引腳，可以用冗餘輸入引腳檢查信號狀態是否正常。

對於模擬 I/O，可以輸入一個恆定電壓，用 AD 轉換，檢查轉換值是否在可接受的較小範圍內。

Class C 認證對策

看門狗、PC 指針、中斷、時鐘、不變記憶體、外部通訊、I/O

採用與 Class B 相同或相似的測試措施。

指令解碼與執行

測試定義：等價類測試(Equivalence Class Test)：預定用於確定是否對指令進行了正確的譯碼和執行的一種系統測試。該測試源自 CPU 指令規範。

認證對策：指令按如下分類：

- 移動指令
- 運算指令
- 位元和移位元指令
- 條件處理指令
- 其他指令

將相似的指令組合在一起，而輸入數據被分成特定的數據區段(等價類)，同組內的每個指令至少處理一組測試數據，以便完整的指令組處理完整的測試數據組。測試數據可由下述內容形成。

- 有效範圍內的數據
- 無效範圍內的數據
- 邊界上的數據
- 極端值和它們的組合

可變記憶體

測試定義：踱步式記憶體測試(Walkpat Memory Test)，一種故障/錯誤控制技術，在這種技術中，標準資料像正常操作一樣被寫入被測儲存區。在第一單元上執行位元反轉，並檢查剩餘的儲存區域。然後，再次反轉第一個單元，並檢查記憶體。對所有被測儲存單元重複該過程。對被測記憶體中的所有單元進行位元反轉，且按上述過程進行第二次測試。該技術識別所有靜態位元錯誤以及記憶體單元之間介面中的錯誤。

認證對策：透明的踱步 1s 和踱步 0s 測試，以及全局變量的動態冗餘校驗。

儲存單元因九宮格內相鄰單元的不同操作導致狀態不正確，這種故障稱為鄰居圖形敏感故障(Neighborhood Pattern Sensitive Faults, NPSF)。造成 NPSF 的主要原因是高密度儲存單元間的相互干擾，檢測 NPSF，實際上也包含了檢測阻塞故障、耦合故障等其他記憶體故障類型。

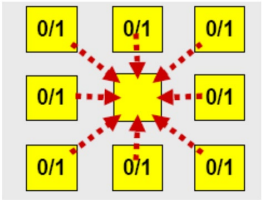


圖 3

踱步 1s 測試，指全部 RAM 設為 0，然後將記憶體的第一個位元組的最高位元設為 1，檢查九宮格內相鄰 bit 是否有變化。然後把 1 右移一位元，重新檢查九宮格其他數據是否有變化，重複右移 7 次，檢查到最低位元。接著檢查下一個位元組的最高位元，依次進行，直到檢查整個 RAM。

在整個測試中，“1”一步一步地從左到右，從上到下，走完整個 RAM。

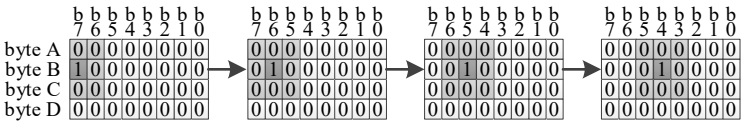


圖 4

踱步 0s，與踱步 1s 類似，指全部 RAM 設為 1，用"0"一步一步地從左到右，從上到下，走完整個 RAM。

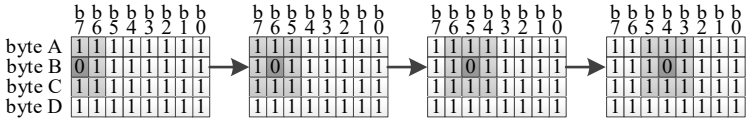


圖 5

與 March 測試一樣，踱步式測試也會覆寫 RAM，破壞原始數據，故也需要將 RAM 做切分，備份數據、踱步測試、恢復數據三步走，實現透明化測試，以及全局變量的動態冗餘校驗，詳細可參考 Class B 的可變記憶體測試章節。

結論

本文根據 IEC 60730 標準與 Holtek 晶片實際情況，推薦了一些對策，利於用戶通過 IEC 60730 認證，並對 IEC 60730 的部分條款與相應的測試對策做了細緻的介紹與解釋，用戶可免去閱讀 IEC 60730 文本並尋找認證對策的過程，可清晰地瞭解的各個測試項目，有針對性地開發自檢程式，加速認證過程。

參考資料

"IEC 60730-1：家用和類似用途的自動電氣控制器" 第 4 版，2009。

HT8 與 HT32 系列 Datasheet 及用戶手冊。

版本及修改資訊

日期	作者	發行
2021.05.18	陳康超(chad)	V1.00

免責聲明

本網頁所載的所有資料、商標、圖片、連結及其他資料等 (以下簡稱「資料」)，只供參考之用，盛群半導體股份有限公司及其關聯企業 (以下簡稱「本公司」) 將會隨時更改資料，並由本公司決定而不作另行通知。雖然本公司已盡力確保本網頁的資料準確性，但本公司並不保證該等資料均為準確無誤。本公司不會對任何錯誤或遺漏承擔責任。

本公司不會對任何人士使用本網頁而引致任何損害 (包括但不限於電腦病毒、系統故障、資料損失) 承擔任何賠償。本網頁可能會連結至其他機構所提供的網頁，但這些網頁並不是由本公司所控制。本公司不對這些網頁所顯示的內容作出任何保證或承擔任何責任。

責任限制

在任何情況下，本公司並不須就任何人由於直接或間接進入或使用本網站，並就此內容上或任何產品、資訊或服務，而招致的任何損失或損害負任何責任。

管轄法律

本免責聲明受中華民國法律約束，並接受中華民國法院的管轄。

免責聲明更新

本公司保留隨時更新本免責聲明的權利，任何更改於本網站發佈時，立即生效。