使用標準接近感測器模組實現安全、可靠的篡改偵測

■作者：Jim Archibald / ams AG

醫療設備、公用事業儀表和許多其他類型的封閉式電子系統，都需要仰賴可靠的方法來偵測未經授權的篡改，並在篡改發生時能夠保護系統及其數據。在醫療設備中，篡改事件導致的儀器效能低落，可能會對患者造成嚴重傷害。在公用事業儀表中，篡改可能是一種欺騙行為，造成公用事業公司的營業損失。因此，在某些產品設計中，可靠、常態性的篡改偵測 (tamper detection) 方法是非常重要的。

在評估篡改偵測的可行方法時，需進行以下的設計考量：

■成本
■裝配程序
■非破壞性或破壞性操作
■被動或主動偵測
■機械或固態技術

不可避免地，某些選擇必須在其他方面有所妥協。然而，在過去兩年，手機大量採用紅外線 (IR) 近接感應，這大大促成了近接感應模組的可用性，同時在效能特性方面也有長足進展，例如更低的功耗和排除光學串擾 (optical cross-talk) 等。這使得整合型紅外感測器模組成為比以往任何時候更具吸引力的篡改偵測選項。本文將比較 IR 解決方案與舊型裝置的特性，並且逐一說明使用商用現成 IR 感測器模組實現篡改偵測電路的步驟。

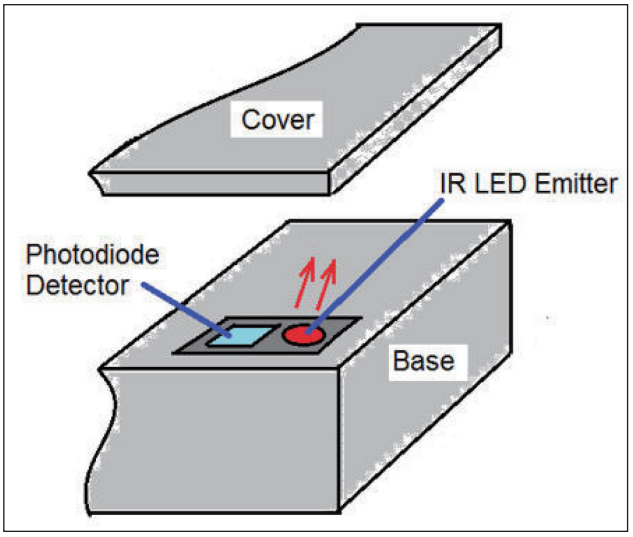
傳統的篡改偵測方法

最簡單的防篡改 (anti-tampering) 解決方案是利用一條導電材料，其完好無損時是完整的電路。打開要保護的設備的蓋子，將電路分開，形成斷路 (open circuit)。透過類比數位轉換器 (ADC)，主控制器可以偵測到斷路並記錄篡改事件。這種方法既簡單又便宜 – 但具有破壞性：在將蓋子放回原位後，防篡改機構依然是斷開的，因此不會偵測到進一步的篡改事件。在大部分產品中，這樣的一次性偵測機制是不夠的。

使用普通的機電開關，這是一個非破壞性的替代方案。在這個方案中，主控制器監測連結至開關的的 GPIO(通用型之輸入輸出) 或 ADC 輸入。如果外殼被打開，控制器會認定開關被切換。相對於破壞性方法，此系統的優點是，在蓋子被移除或發生篡改之後，外殼可以重新安裝，且開關能重設為預設狀態。

使用機械開關的主要缺點，在於它容易受到大氣中氧氣和濕氣的氧化和腐蝕。隨著時間推移，腐蝕會導致金屬開關卡在某個位置，如此一來，當蓋子移動時，開關無法切換。特別是對於預估使用壽命長達多年的公用事業儀表等產品來

圖 1：外殼由底座和蓋子構成。IR LED 發射器和光電二極體偵測器被安裝在底座上，時時偵測蓋子是否移位。



說，這樣的機械開關是不適用的。

相對地，使用固態技術則能實現永久免受腐蝕且非破壞性的篡改偵測電路。圖 1 顯示這種採用 IR LED 發射器和光電二極體偵測器的解決方案。當底座和蓋板組裝到位時，蓋子上的反射片或其他障礙物會覆蓋光電二極體偵測器。底座的接近感測器將定期點亮以檢視蓋子是否仍在原來的位置。如果光電二極體偵測到自 LED 反射的光的強度高於特定數值，則表明蓋子是在原位。當蓋子移動時，入射到光電二極體的光線強度將急劇下降，這會啓動感測器記下可能的篡改事件。

這種方法是非破壞性的：IR LED 和光電二極體被安裝在底座上，無論蓋子是在原位還是已經被移動，只要它們和系統電源保持連接，就可以持續工作。

這種解決方案的機械設計和組裝很簡單，因為只有底座需要電路，蓋子部分不需要電路。這和另一種使用磁開關的非接觸式偵測方法截然不同，磁開關方式需將永磁體 (permanent magnet) 安裝在蓋子中，並與底座中的開關對齊：在這個方案中，移動蓋子會削弱開關所暴露的磁場，進而觸發警報。這種磁性方法的組裝更為複雜，並且有著被雜散磁場干擾的風險。

在 IR 感測器電路中，調變 IR LED 發出的脈衝有其用處：光電二極體可以被設定為能辨識 LED 的特殊調變方式。這讓光電二極體可以區分 LED 發出的光與周圍的紅外光源，例如太陽光，如此就能避免因受到光線干擾而無法偵測篡改事件的風險。對任何篡改者而言，這種主動的篡改偵測機制 1 也多加了一層障礙，因為篡改者無法僅利用標準 IR 光源的光來照射就能破解感測器。

使用整合型接近感測器模組，例如奧地利微電子 (ams AG) 的 TMD2620(ams.com/eng/Products/Light-Sensors/Proximity/TMD2620) 可以實現非破壞性的主動篡改偵測系統。此模組將 IR 二極體發射器和光電二極體偵測器結合在一個封裝中 (見圖 2)。類似的近接模組被用於許多智慧型手機顯示器的背光調光控制電路中當智慧型手機在通話期間靠近使用者臉部時，接近感測器能啓動系統調暗螢

圖 2：整合型 IR 接近感測器模組 TMD2620 的區塊圖

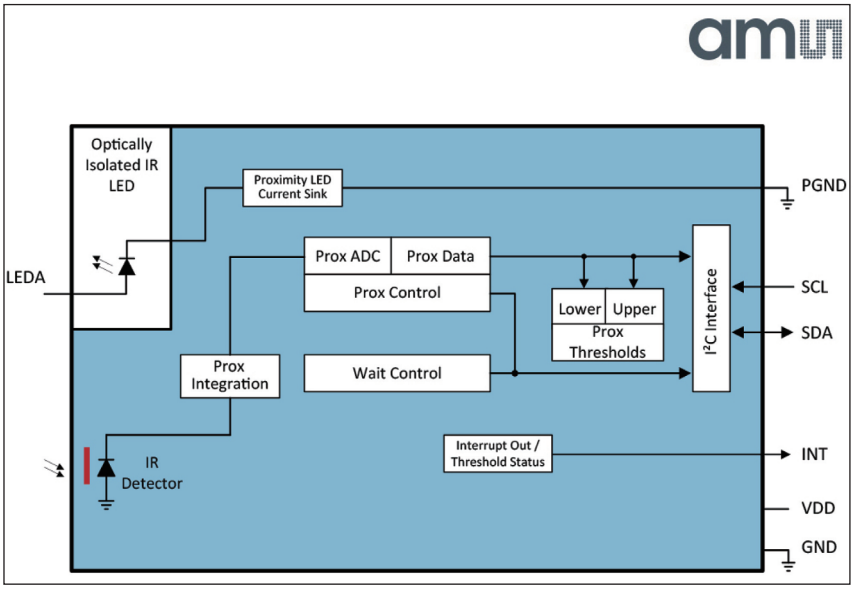
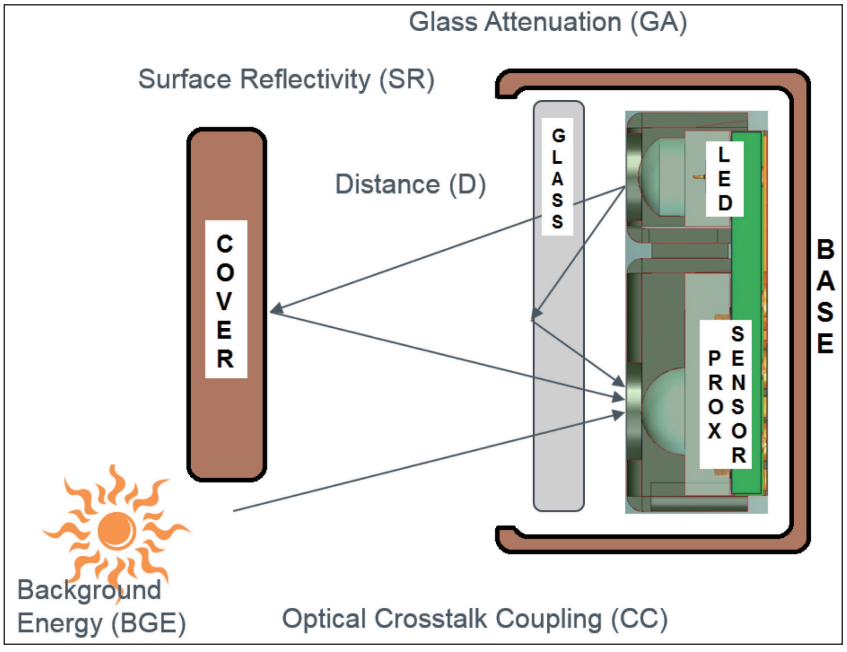


圖 3：近接感測系統內的光學反射



幕，如此能節省功耗、防止雜散光線射進使用者的眼睛，且能停用螢幕的觸控感測器。在大量手機市場中，感應模組已被廣泛使用，因此其成本近年來大幅下降。最新感測器模組的平均功耗也比以前的型號低得多。

小型 TMD2620 模組 (3.1mm x 2.0mm x 1.0mm) 包含一個 I²C 介面，幾乎能與任何微控制器通訊。LED 的脈衝輸出可以設定各種輪詢 (polling) 和定時模式及頻率。

附錄：用於篡改偵測應用的主微控制器代碼範例

via I²C interface Configuration

Write 0x80 0x01 // turn on device

// set proximity parameters

Write 0x8e 0x00 // Use 4?s pulses with 1 pulse per pulse train

Write 0x8f 0xc0 // set proximity gain=8x, LED drive current=6mA

// set wait time to 8.65s

Write 0x8d 0x84 // Set wait time cycle length

Write 0x83 0xff // Set wait time to maximum number of cycles

// (total wait time between readings = 8.65s)

// configure interrupts

Write 0xdd 0x20 // Enable proximity interrupt

Write 0x88 0x8f // Set low threshold. Interrupt pin will be asserted when prox

// reading goes below 0x8f in this example.

Write 0x8a 0xff // proximity high interrupt threshold

Write 0x8c 0xf0 // Proximity interrupt persistence:

// interrupt will fire after 15 consecutive prox values outside the range

// begin proximity operation

Write 0x80 0x0d // enable wait, prox detection

Inside the Interrupt Service Routine:

Read 0x9c // gives proximity data

參考：

1) http://www.edn.com/electronics-blogs/beyond-bits-and-bytes/4391255/Don-t-trust-your-tamper-detection-circuitry--it-may-be-dumb-

概述

醫療設備、公用事業儀表和許多其他類型的封閉式電子系統，都需要仰賴可靠的方法來偵測未經授權的篡改，並在篡改發生時能夠保護系統及其數據。在醫療設備中，篡改事件導致的儀器效能低落，可能會對患者造成嚴重傷害。在公用事業儀表中，篡改可能是一種欺騙行為，造成公用事業公司的營業損失。因此，在某些產品設計中，可靠、常態性的篡改偵測 (tamper detection) 方法是非常重要的。

在評估篡改偵測的可行方法時，需進行以下的設計考量：

■成本

■裝配程序

■非破壞性或破壞性操作

■被動或主動偵測

■機械或固態技術

不可避免地，某些選擇必須在其他方面有所妥協。 然而，在過去兩年，手機大量採用紅外線 (IR) 近接感應，這大大促成了近接感應模組的可用性，同時在效能特性方面也有長足進展，例如更低的功耗和排除光學串擾 (optical cross-talk) 等。這使得整合型紅外感測器模組成為比以往任何時候更具吸引力的篡改偵測選項。本文將比較 IR 解決方案與舊型裝置的特性，並且逐一說明使用商用現成 IR 感測器模組實現篡改偵測電路的步驟。

使用模組而非離散式 LED 和光電二極體的優點在於：ams 封裝提供了最佳化的光學路徑，可將串擾保持在非常低的水準 (串擾來自於 LED 玻璃蓋至光電二極體的內部反射)。圖 3 顯示可能影響接近感測器操作的各種光學反射。

此外，上述基於 IR 模組的設計擁有極長的預估使用壽命，並且不需承受腐蝕風險及機械式開關故障所帶來的麻煩。現成的近接模組可以加快產品上市速度，且較離散式設計更易於實現。

當然，採用機械開關的電路或導電材料帶的優點是易於實現，而紅外近接感應解決方案也具有同樣的優點嗎？

下面所示為偽代碼 (pseudo-code)，可由系統主微控制器運行以設定 TMD2620 模組的內部註冊器。這指明要讓 TMD2620 篡改偵測系統正常運行所需的編碼範圍。

第一步是讓 MCU 透過寫入”啓用”註冊器 (0x80) 來啓動接近感測器。啓用該裝置意謂 IR LED 可以開始與光電二極體 IR 偵測器同步發射 IR 脈衝。

光電二極體的光強度測量值由 TMD2620 中的 ADC 轉換為數值。這些讀數會隨著時間而累積。如果積分值在給定的時段內超過了特定閾值，則外殼的底座和蓋子會被判定為彼此靠近，這就表示沒有遭到篡改。

系統的功耗與 IR LED 發光的頻率成正比。在下面的代碼範例中，等待時間註冊器 (wait time registers) 由主微控制器設定為 8.65 秒：每 8.65 秒 (最大可能間隔) 執行一次近接讀取，這樣的頻率對許多應用已是足夠的，因為它假設有人想篡改該產品時，移除蓋子的時間不可能短於 8.65 秒。

TMD2620 包含一個近接中斷位元 (proximity interrupt bit)，當偵測到一個靠近的物體時，該位元就會作用。下限和上限閾值分別由註冊器 0x88 和 0x8A 設定。

持續性濾波註冊器 (0x8C) 僅在發生一定數量的連續讀數高於期望閾值之後，才會允許產生中斷。

“狀態”註冊器 (0x93) 包含近接中斷位元 (位元 5)。當感測到模組附近的物體時，該位元會作用。中斷位元可以被設定為在執行狀態註冊器讀取時自動歸零。無論何時當近接中斷作用時，系統 MCU 通常會運行中斷服務程序 (ISR)。然後，ISR 將檢查近接數據註冊器 (0x9C) 以查看積分值是否呈現較大值 (表示底座和蓋子仍然連接)。另一方面，較小的數值則表明底座和蓋子已經彼此分離，換句話說，可能發生了篡改事件。

MCU 可以記錄顯示篡改事件發生的時間戳記，並測量其持續時間。近接中斷是一個很便利的功能，因為它可以減輕 MCU 管理輪詢感測器程序的需求。近接中斷是 TMD2620 簡化主控制器操作的另一種方式。

在上述的設定中，LED 在 8.65 秒的時間間隔內將以 4μs 的周期消耗 6mA 電流。這表示 IR LED 的平均電流消耗為 2.77nA。當電源開啓時，整個模組的一般功耗約為 30μA，讀取數據時則會多一些。

結論

使用 IR LED 感應模組實現篡改偵測，就機械方面而言是很容易的，因為它只會影響成品外殼的一面。IR LED 感應模組還提供無損操作 (non-destructive operation)、抗腐蝕和支援主動監控等優點。

IR LED 輸出的調變消除了環境光線干擾的風險，並且可以持續、可靠地偵測蓋子與底座之間是否分離。

作者簡介

Jim Archibald 的工作地點位於德州普萊諾市，他負責管理奧地利微電子 (ams AG) 的美國現場應用工程師團隊。他曾擔任硬體設計及數位信號處理、市場行銷和銷售方面的開發和工程管理職務。Archibald 擁有普渡大學電機工程碩士學位，他是一位具有執照的專業工程師 (PE)。他擁有八項美國技術發明專利。

For further information

ams AG
Jim Archibald
Senior Manager, Field Applications Engineering
Tel: +1 610 360-7254
Email: Jim.Archibald@ams.com
www.ams.com
info@ams.com CTA