

對精確度錙銖必較的物聯網

■作者：Grainne Murphy 及 Colm Prendergast/ADI 公司

物聯網 (IoT) 簡單地說，就是將任何具備感測器或控制器的裝置設備，連接到網際網路 (和 / 或這些連接設備之間彼此連接) 的一種概念。這包括了從手機、電器設備、汽車、機器、機器的元件、穿戴式設備、乃至於任何其它我們可想到的物件。而物聯網的原理，實際上就是一個連接並延伸到雲端的量測信號鏈。

感測 / 測量元件首先將類比信號轉換為數位數據流，此數位格式接著便可進行擷取、處理、轉換、分析，然後再基於結果做出判斷。將光、聲音、壓力、和溫度等物理現象轉換為數位資料，其實已經是很老舊的概念。物聯網的演進，已經透過 metapatterns(元式樣)，以及雲端與其龐大的儲存和處理能力所實現的運算模型力量，轉變了基於此數位資料所做出的決定。一些如溫度測量技術的傳統

感測能力，大家都已可充分理解，並普遍被用於獨立的測量和其他感測的元素之一。比方說，在電化學感測中，溫度會影響到量測結果，就必需要加以考慮。另一方面，也有一些更新穎且讓人感到興奮的感測器發展，將可對物聯網世界產生巨大的影響。

其中一個例子是 MEMS 加速度感測器，這類感測器是多軸振動偵測的組成基礎，藉以實現系統的穩定化，如無人機、手持式遊戲裝置、或是相機等。振動偵測也被運用於健康追蹤設備中，藉以測量出個人的健康狀況。健康和健身用的穿戴式感測器必需長時間開啓，並進行高精確度的人體運動偵測，以便加以進行分析 - 如跑步、騎自行車、或步行 - 並將即時數據傳送到各類的行動式健康和健身應用裝置上。

圖 1：從感測器到雲端的信號鏈。

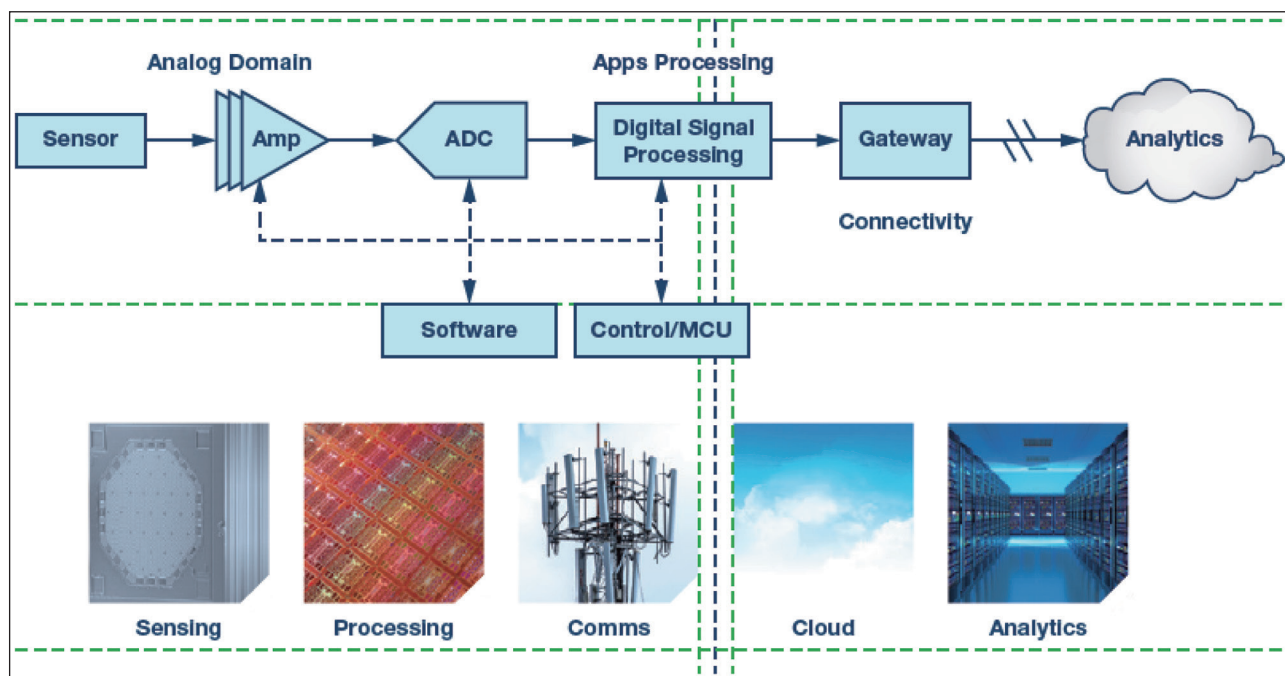
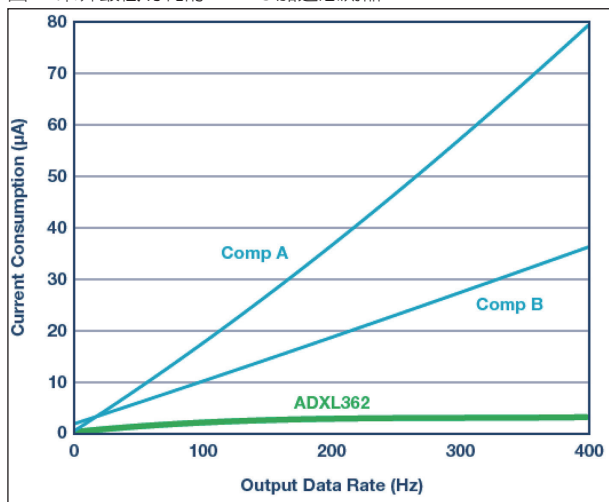


圖 2：業界最低功耗的 MEMS 加速感測器。



以加速感測器為例，在一個物聯網裝置中我們應該尋找怎樣的產品？而更準確的測量所代表的價值又是什麼呢？首先就是要考慮低功耗。ADI 的 ADXL362 是一個超低功耗的 3 軸 MEMS 加速感測器，在 100Hz 的輸出數據速率下，其消耗電流小於 $2\mu\text{A}$ ；而在運動觸發喚醒模式下（由 MEMS 加速感測器量測加速度的靜態或動態力量），電流則小於 270 nA，藉此可延長電池的壽命。其次要考慮到帶寬和解析度，ADXL362 不會有過低採樣 (under sampling) 所產生的輸入信號混疊 (alias) 問題，它能以所有的資料速率對感測器的完整頻寬進行取樣，並具有低雜訊的效果，藉此實現最小信號的量測。對於那些雜訊位準需求低於 ADXL362 正常值 $550\mu\text{g/Hz}$ 的應用而言，則有兩種較低的雜訊模式（低至 $175\mu\text{g/Hz typ}$ ）可供選擇（在電源電流最小增加的條件下）。

更好的品質數據很重要：

但是，這種精密測量的價值究竟是什麼，又為何有其重要性？低雜訊、低漂移的元件能將感測器的能力加以最大化，實現更寬的動態範圍，這也意味著此硬體能量測更多樣的小信號。這讓終端系統可更準確、靈敏、且差異化。而準確性的提高，將有助於開發出能夠滿足目前已被提出及尚未被提出的量測要求，同時並具有符合未來需求空間的平台

硬體。

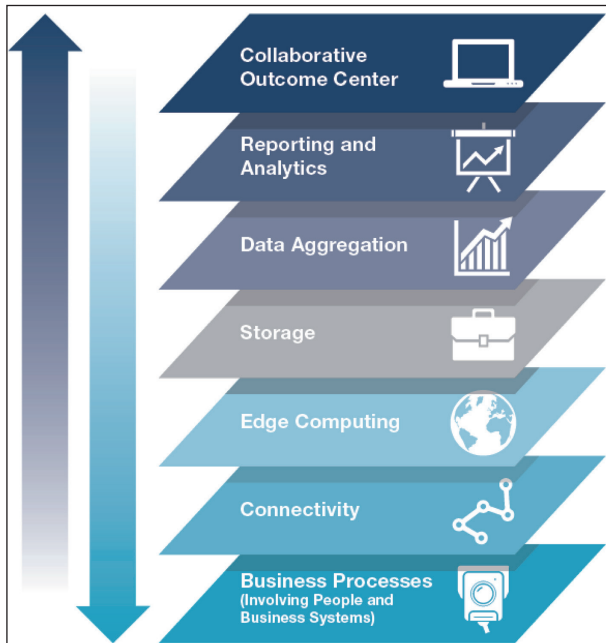
如此一來，同樣的硬體可被用於具有低成本優勢的多代產品上，特別是在硬體更換升級實施困難且昂貴的情況下。這點對於物聯網來說，由於其感測器及相關的硬體預期將有數量上的爆發成長，將特別適用。根據市場分析公司 Gartner 的預測，到 2020 年時，將會存在超過 260 億個相互連接的裝置 – 這代表著一個很龐大的連接數量。此外，由於物聯網信號鏈中使用無線連接的優勢，這些裝置將可被放置於越來越難以觸及或惡劣的環境中（如工廠）。最後，另一個可能要考慮的因素，是越來越嚴格的跨市場政府法規，包括氣體排放、電力使用、和環境控制等。更優良的測量系統能提供前瞻性的思維，以滿足這些可能新出現和被改變的法規，這需要在既有硬體內進行更精確的量測。能夠滿足未來的新測量需求，就等於是確保了差異特性，能在勢必將十分擁擠與競爭的物聯網市場中生存下來。

因此，穩定而精確的硬體測量平台的重要性是不容置疑的。當此平台設置完成後，可以再透過軟體來實現系統的差異化。在物聯網中，這樣的功能已被證明，是一個在此競爭激烈的市場中讓各家公司能夠進一步區隔自己的領域。此外，任何系統升級也將會更容易、更簡單、且可以即時地完成。

合法 (legitimate) 數據很重要性

要確保在物聯網生態系統中維持數據的合法性，需要考慮到很多的因素。物聯網可被解釋為數個階層，從“物”一直到雲端。在每一個階層中，都可能有一個新的外部連接及其相關的安全風險。還有一個可能的返回路徑 (return path) 通過層回到“物”。這不僅是關於裝置設備、網路、或客戶端 – 而是涉及到許多表面區域 (surface areas)，且每一個還可以互連。舉例來說，從裝置設備到雲端，或是從裝置設備到閘道器再到雲端。而合法性的目的就是要確保每一階層的安全，當我們連接越多的物、雲端、和閘道器時，我們也同時增加了易受安全漏洞所影響的地方。

圖 3



由 OWASP(Open Web Application Security Project, 開放網路安全研究計畫) 所整理出來的前 10 大物聯網安全漏洞為：

- 不安全的上網路界面 (XSS, 灌入, 網路釣魚)
- 不足的身份驗證 / 授權
- 不安全的網路服務 (SSH, SFTP, Telnet)
- 缺乏傳輸加密
- 隱私問題 / 疑慮
- 不安全的雲端介面
- 不安全的手機界面
- 不足的安全可設置性
- 不安全的軟體 / 韌體
- 不佳的實體安全性 (physical security)

在雲端中, 安全威脅可以是資料洩露, 但也可以是意外的資料遺失或資料竊取。毫無疑問的, 雲端服務必然會同時對應多個客戶 (多租戶), 因此其服務需要能確保從一個客戶到另一個客戶之間的安全切割 (secure segmentation)。接下來還有一些其他問題也需要考慮, 包括系統的可用能力 (availability capabilities) 為何, 以便在可能的數據失效情況下, 保持本地上線 (online locally) 或做其他處理? 如何在多個地點共享並保護資料, 以及安

裝了哪些安全標準? 是否可以備份資料, 特別是當物聯網造成的資料量爆炸時? 此外, 多用戶使用的應用程式介面 (API), 將會透過相同的雲端服務被開發與儲存, 因此, 如何執行身份驗證和授權 (以及如何保護特權用戶, 如管理員) 將會非常地重要。

審查和評估雲端服務供應商的方法很多, 其中的一種機制, 是透過其發行的安全準則。這類全球雲端的指導準則, 目前正不斷地被擴充改進中, 而服務供應商也將越來越會被要求須取得相關準則的符合認證。

但事實上安全問題並不僅限於在雲端上, 在階層堆疊中的每個層別都有其相關的威脅和技術對策。實體物聯網設備和閘道器可能會被竊取或篡改, 讓資料被未經授權的用戶操縱或存取。對於這類問題, 採用的對策為篡改檢測器 (tamper detectors)、加密技術 (cryptography)、或裝置設備的註冊。軟體或韌體都有可能成為網路釣魚、惡意軟體攻擊、或操縱的目標。在這類的場合中, 可靠的作業系統、將安全性建立於開發生命週期中、以及安全漏洞測試等, 就顯得非常的重要。設備被部署到現場之後, 提供一機制來安全地更新軟體也很重要。當資料被傳送時, 不安全的通道可能會遭致操縱、竊聽、或攻擊。對此, 加密的傳輸通道、埠 / 介面的管理、以及持續的主動監控會是關鍵。對於資料的隱私, 客戶的信心需要特別重視, 即使是最小的資料洩漏, 都可能造成公司品牌和聲譽上的損害。因此, 一些良好的做法, 像是採用資料加密技術來將被儲存的資料最小化或模糊化, 以及資料的保留都是很重要的。由於全球的隱私資料政策正持續地演進和變化中, 具有一靈活的系統, 以便能基於全球的不同區域來處理法規差異以及共識, 是很重要的。在應用程式的層次上, 不僅僅是靠用戶身份驗證和授權來阻止未經授權的資料存取, 還必須持續不斷地測試程式碼的漏洞。另外, 還要考慮帶外 (out-of-band) 保護, 如 WAF(web application firewalls, 網際網路應用程式防火牆) 以及隔離和閉鎖受到攻擊的帳戶的能力。這裡所介紹的所有對策都值得考慮採用,

但更重要的是，安全性必須是被”設計”到環境系統中，而不是到了最後關頭才來加以修正。

智慧型連接的物聯網系統

智能 (或資料處理) 可以被加入於物聯網鏈中的任何階段。舉例來說，在生命體徵監測 (VSM) 中，當身體溫度處於危險位準的即時警報，可直接在感測器上發生時，就沒有需要將體溫數據發送到雲端；不過，此溫度數據也可以被用於其他生物醫學資料運算上，因此它還是可以被用在閘道器或雲端中。

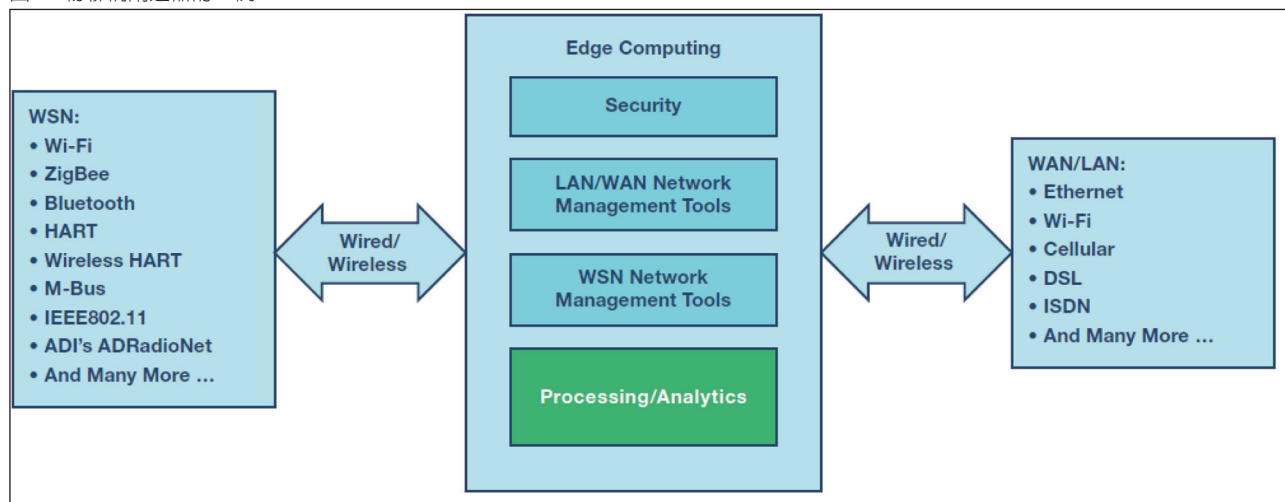
當信號處理在節點處進行時，會有若干優點，其中包括能實現緊密且整合的回授控制迴路。緊密耦合到感測器和 / 或致動器所帶來的好處，在於能立即做出決定。例如，一達到預定位準的振動可讓機器或馬達立即斷電，或是一溫室中的溫度升高可以驅使馬達打開窗戶。對於節點的需求，需同時包括較小的佔用空間，以及能實現盡可能長電池壽命的最低功耗。而像是 ADI 的集成式類比微控制器元件 ADuCM360 (結合了 ARM M3-MCU 和 24 位元類比數位轉換器)，正可以實現這些需求。在未來，可使用採集能源 (harvested energy) 的能源獨立裝置設計，將會是成功的關鍵。節點處理的限制，在於空間和電力限制，此外也很難整合其他資料來源上的數據。另外，節點處的低功率會限制資料傳輸範圍和有效載荷 (payloads)。由於節點管理上存在

著狀態監控和執行升級的困難，因此會造成網路邊緣上的實體、軟體、和資料安全風險。

基於閘道器 (gateway-based) 的信號處理，使用的是一端連接到短距離無線感測器網路 (WSN)，而另一端為 LAN 或 WAN 連結的物聯網閘道器設備。它類似於路由器，也可以做為感測器的集線器 (hub)。除了 WSN 網路管理和安全功能，它通常也被用來作為本地處理和分析 (通常稱為邊緣運算) 的運算資源。基於閘道器的信號處理，其優點為潛在的大量處理資源，這些資源能夠整合來自其他感測器 / 來源的數據。因此，能夠進行靠近網路邊緣分析的能力，以及可藉由現成的開發工具來開發這些分析功能，兩者的結合將可提供一項更加 IT 友善的解決方案。它具有成為全端 (full stack) 作業系統的潛力，並使用更高安全標準遠程管理工具的 LAN/WAN 網路技術 (雖然實體安全可能是一種風險)。但從另一個角度來說，它通常不是低功率，需要搭配有線的電源，且其資料儲存是有限制的。

因此，雲端連接的主要優勢之一，是能夠使用歷史數據和 / 或來自多個設備的數據，進行大筆資料記錄儲存、取得、和搜索的能力。對於基於雲端的信號處理而言，在許多情況下，資料儲存與大數據處理 / 分析之間密切相關。而它不僅有足夠儲存資料數據，其能夠快速存取和處理資料的需求，驅使產生許多創新方法，而這些方法使用具有開源框架的簡單編程模型，來實現跨電腦群的大型數據

圖 4: 物聯網閘道器的一例



集的分散式處理。基於雲端的處理，其明顯優勢在於具有內建安全性且潛在非常龐大的運算與儲存資源。此外，有種類眾多且不斷增加中的開源及商用開發工具，以及終端解決方案可供輕鬆使用。

軟體即服務 (Software as a Service, SaaS) 被認為是目前雲端運算中的關鍵產品，其他還有基礎架構即服務 (IaaS)、平台即服務 (PaaS)、桌面即服務 (DaaS)、行動後端服務 (BaaS)、以及資訊技術管理即服務 (ITMaaS) 等。這些服務提供了各種的選項，以適應終端系統的需要。對於基於雲端的信號處理而言，需要服務器託管 (可以在同建築內部或遠端)。就通信和大型數據儲存來說，儲存和服務的相關成本可能會很昂貴。其他的缺點還包括網際網路通信通道在延遲和傳輸量上的不可預測性。

隨著物聯網系統的發展，智慧型系統的區隔方式也同樣在變化，讓更多的智慧功能移往節點。如果不在節點上加入智能和知識，就意味著數據即單純只是數據，直到它到達雲端為止，但雲端上所有數據的轉換及發送都是高耗電且佔用大帶寬。在智慧型智能感測中，節點會將數據轉換為可降低總功耗、降低延遲、並減少帶寬浪費的資料。簡單地說，這有利於從反應式 (reactive) 物聯網移往預測和即時式 (predictive and real-time) 物聯網。

要設計出優秀的物聯網所需面對的挑戰非常

多，包括良好的測量、安全性、以及要了解在整個物聯網路徑中有效使用智能的地方。此外，可能有一些完整物聯網解決方案的供應商，來自於感測器、閘道器、軟體、和儲存設備供應商。在 ADI，我們同時是物聯網供應商和客戶，我們使用自家的 ADXL362 加速度感測器 (在其他用來測量溫度和濕度的感測器) 來監控我們位於 Limerick 廠區的製造設備。透過測量機器或馬達的振動模式變化，可以在系統失效之前檢測出故障。這具有能夠規劃預測性維修計畫的優點，從而提高工廠效率和產能。ADI 的物聯網實現，能夠在複雜的製造過程中，為多台設備 (無論新舊以及來自不同供應商) 提供了一個完整的監控與分析系統。此系統能即時追蹤及回報效率，並在系統故障前提醒技術人員可能出現的問題。此作法提高了晶圓的產出量，且由於能針對我們的客戶的終端需求提供更穩定的供應量，因而有助於他們進行更好的計劃，此實例顯示出了物聯網系統的真正價值。物聯網系統的複雜精密性和涵蓋範圍，提供了許多的信號處理選項。將物聯網系統中的信號處理從雲端移往邊緣，能讓更高智慧度的感測器和資訊提取作業更接近於來源處。網路邊緣節點、閘道器、以及雲端上的可用處理資源，提供給系統設計者得以進行邊緣節點功率、資料頻寬、運算、和儲存需求之間，妥協方案優化的能力。CTA

COMPOTECHAsia 臉書

每週一、三、五與您分享精彩內容

<https://www.facebook.com/lookcompotech>