CTIMES
零組件雜誌 COMPONENTS & CONVERGENCE Jul.333


P.20
前行政院長張善政

次世代封裝技術

產業觀察

獨賣價值

專題報導

ISSN 1019-8628
CTIMES
CTIMES
定價180元

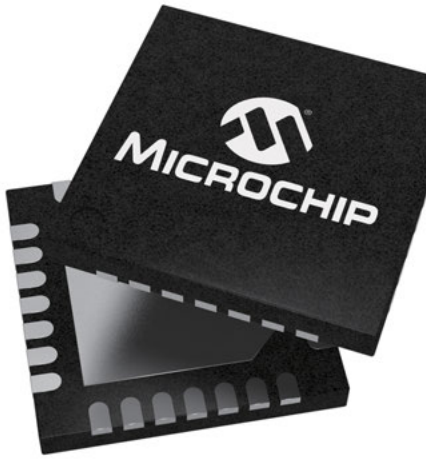

現貨且準時
全球最豐富的電子元件品項
可立即出貨™
訂購滿新台幣 1400 元
或美元 50 元
免運費
0080-185-4023
DIGIKEY.TW
Digi-Key
ELECTRONICS
線上供應超過 770 萬種產品 | 超過 800 家業界領導供應商 | 100% 授權經銷商
*低於新台幣 1400 元的所有訂單將收取新台幣 600 元運費。低於美元 50 元的所有訂單將收取美元 20 元運費。所有訂單將透過 UPS 運送，在 1 至 3 天內送達（視最終目的地而定）。無任何手續費。所有費用將以新台幣或美元計價。Digi-Key 是所有合作供應商的授權經銷商。每天新增產品。Digi-Key 和 Digi-Key Electronics 是 Digi-Key Electronics 在美國及其他國家的註冊商標。
© 2019 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA
ECIA MEMBER
Supporting The Authorized Channel

維護您的智慧財產、品牌和營收

易於加入且難以破解的安全解決方案

讓 Microchip 協助維護您的設計、品牌以及營收。憑藉二十年的在安全設計上的經驗，我們的專家能夠消除您對整合安全措施的擔憂，無需高薪聘用內部專家。將這些專業知識與我們的安全的生產機制和佈建服務結合，您就會瞭解為何許多頂尖公司都信任 Microchip 的專家，協助指導其設計。

從安全加密到信任的執行環境，藉由我們一系列硬體和軟體型解決方案，找到符合您獨特需求的安全措施實施方式。



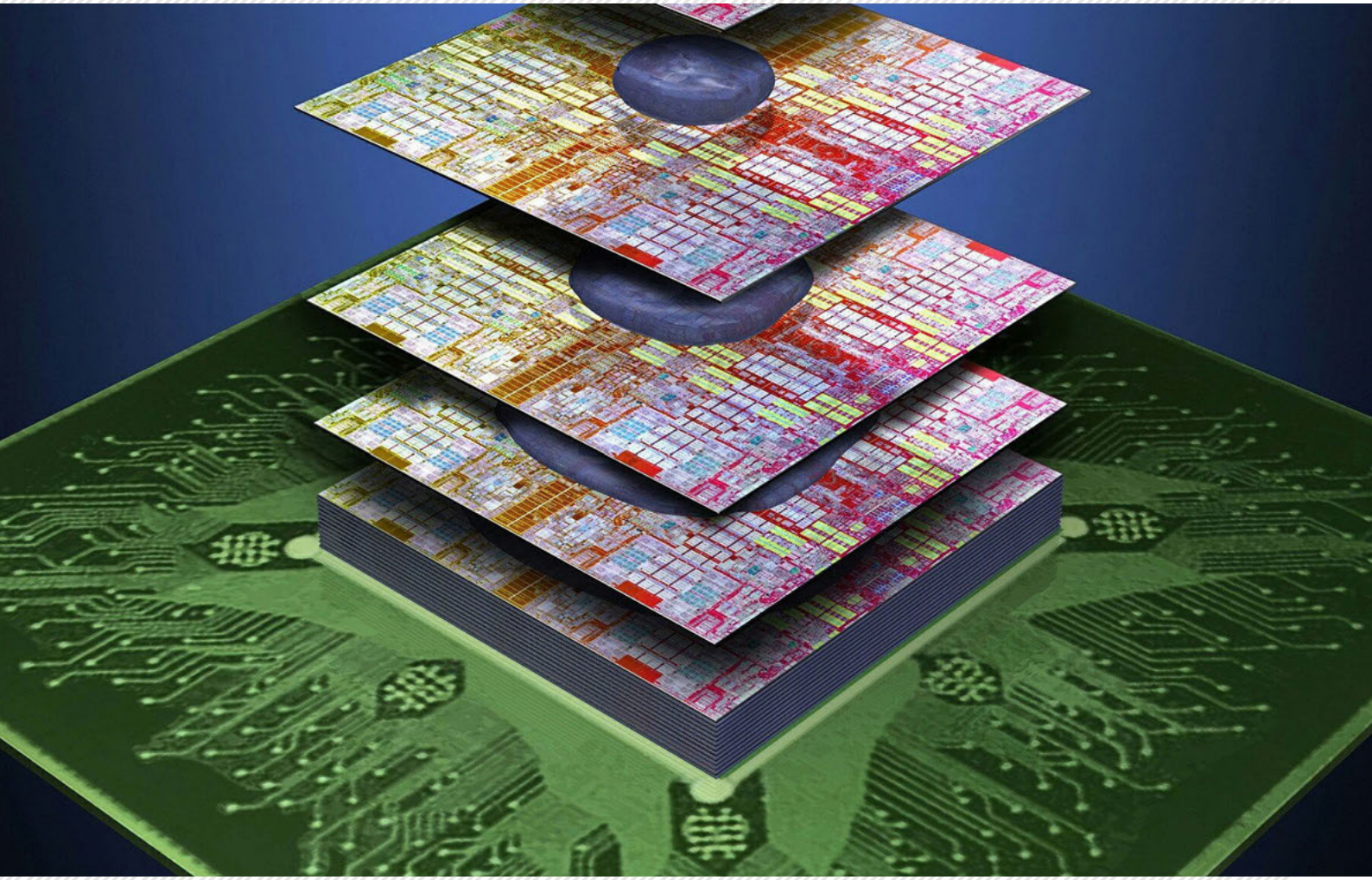
聯繫信息
Microchip 台灣分公司
電郵：rtc.taipei@microchip.com
技術支援專線：0800-717-718
聯絡電話：
- 新竹 (03) 577-8366
- 高雄 (07) 213-7830
- 台北 (02) 2508-8600

保護您的設計，請參閱
microchip.com/Secure

SMART | CONNECTED | SECURE

MICROCHIP

CONTENTS



封面故事

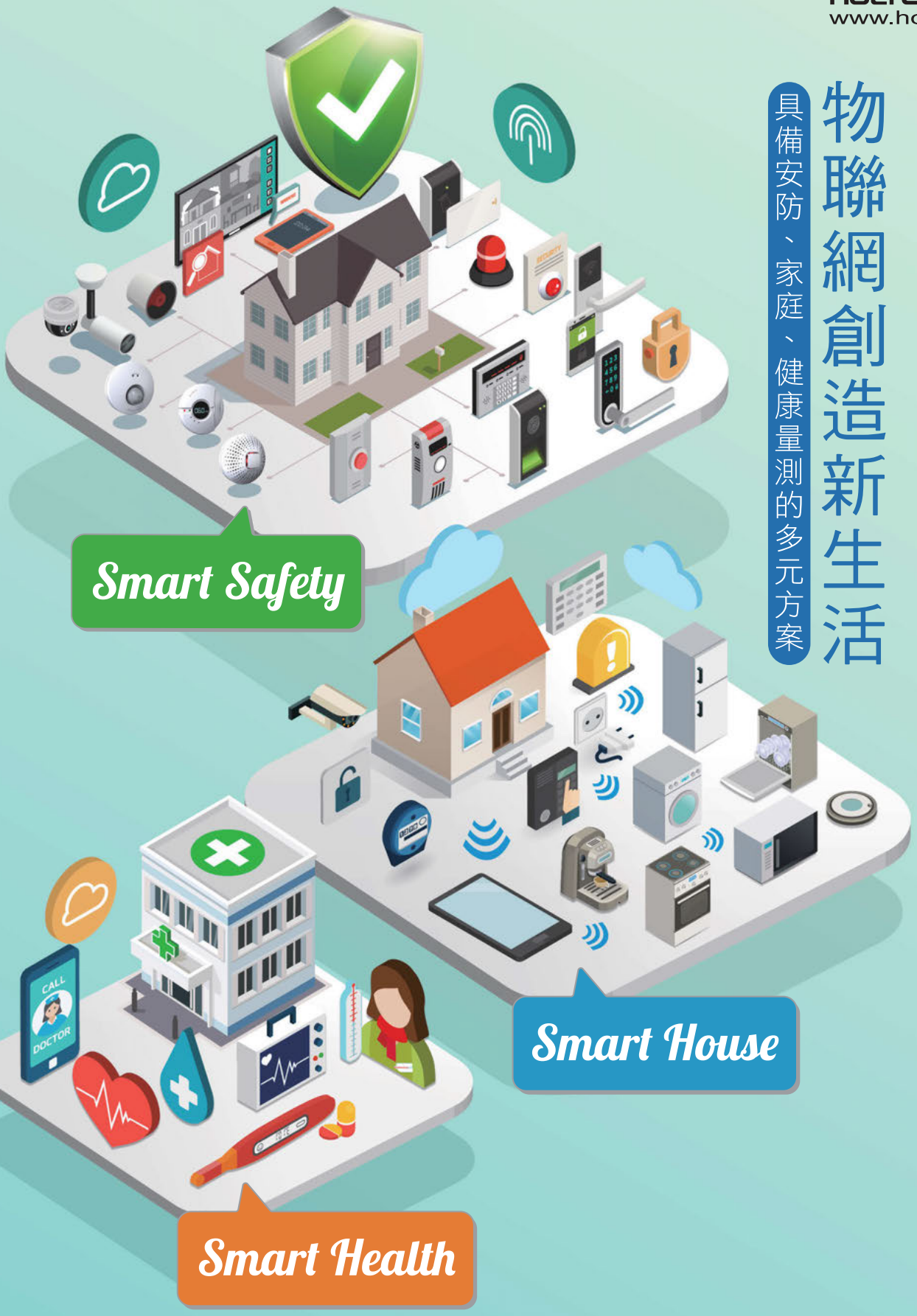
編者的話

新聞分析

HOLTEK
www.holtek.com

物聯網創造新生活

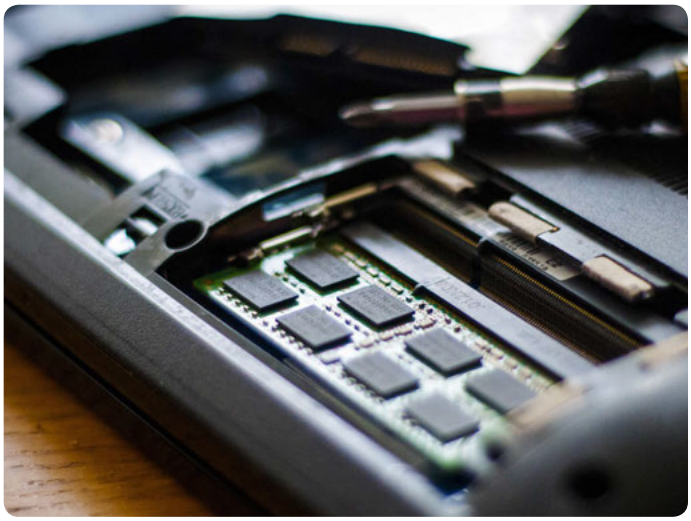
具備安防、家庭、健康量測的多元方案



盛群半導體股份有限公司
HOLTEK SEMICONDUCTOR INC.

總　公　司　新竹市科學工業園區研新二路3號　TEL : 03-563-1999　FAX : 03-563-1189
台北營業處　台北市南港區園區街3之2號4樓之2　TEL : 02-2655-7070　FAX : 02-2655-7373
合泰半導體(中國)　中國東莞松山湖新竹路4號新竹苑10幢(總部壹號10號樓)　TEL : 86-769-2626-1300　FAX : 86-769-2626-1311

CONTENTS



megawin

ARM Cortex-M0
MG32F02系列

漏電斷路保護器

電池管理系統

工業儀表

電梯控制

特性

- ●外接存儲器總線
  EMB (External Memory Bus)
- ●直接記憶體存取
  DMA (Direct Memory Access)
- ●迴圈冗餘校驗
  CRC (Cyclic Redundancy Check)
- ●數位類比轉換器
  DAC(Digital-to-Analog Converter)

後發先至，淩(M0)駕齊驅

Item	Vdd	Flash ROM	Data RAM	Max. Freq.	Timer (16-bit)	IO	ADC	Comp.	Inter-Face	CCP*5	ISP/IAP	Package
**MG32F02A032*1	1.8V~5.5V	32KB	4096B	48MHz*2	5+RTC	44/29/17	12-Bit, 12-CH	2	UART*3 x2, I²C SPI/QPI/PWM CRC, DMA	4-CH	YES*4	TSSOP20, QFN32, LQFP48
**MG32F02A064*1	1.8V~5.5V	64KB	8192B	48MHz*2	6+RTC	44/60	12-Bit, 16-CH	3	UART*3 x3, I²Cx2 SPI/QPI/OPI CRC, DMA, DAC	6-CH	YES*4	LQFP48, LQFP64
**MG32F02A128*1	1.8V~5.5V	128KB	16384B	48MHz*2	5+RTC	44/60	12-Bit, 16-CH	4	UART*3 x4, I²Cx2 SPI/QPI/OPI CRC, DMA, DAC	8-CH	YES*4	LQFP48, LQFP64
MG32F02A072*1	1.8V~5.5V	72KB	8192B	48MHz*2	7+RTC	44/59	12-Bit, 16-CH	4	UART*3 x4, I²Cx2 SPI/QPI/OPI EMB, CRC, DMA PWM, DAC	8-CH	YES*4	LQFP48, LQFP64
MG32F02A132*1	1.8V~5.5V	132KB	16384B	48MHz*2	7+RTC	59/73	12-Bit, 16-CH	4	UART*3 x4, I²Cx2 SPI/QPI/OPI EMB, CRC, DMA PWM, DAC	8-CH	YES*4	LQFP64, LQFP80
**MG32F02U064*1	1.8V~5.5V	64KB	8192B	48MHz*2	6+RTC	44/60	12-Bit, 16-CH	3	UART*3 x3, I²Cx2 SPI/QPI/OPI USB, PWM CRC, DMA, DAC	6-CH	YES*4	LQFP48, LQFP64
**MG32F02U128*1	1.8V~5.5V	128KB	16384B	48MHz*2	6+RTC	44/60	12-Bit, 16-CH	4	UART*3 x4, I²Cx2 SPI/QPI/OPI CRC, DMA, DAC	8-CH	YES*4	LQFP48, LQFP64

**Under Development *1Support M-LINK ICE *212MHz and 11.059MHz as internal RC oscillator, used 12MHz as default. Frequency deviation: at25°C,under ±2.5%
*3All UART support SPI Master *4Share with all Flash zone *5CCP: Input Capture/ Output Compare/ PWM

臺灣總公司
笙泉科技股份有限公司
新竹縣竹北市台元一街8號7樓之一
TEL:886-3-5601501
E-mail: sales@megawin.com.tw

笙泉科技 (深圳) 有限公司
深圳市福田區車公廟泰然九路海松大廈B-905
TEL:86-755-8343-5163
E-mail: sales@megawin.com.tw

CONTENTS

CTIMES 零組件雜誌
Founded from 1991

社長 / 黃俊義 Wills Huang

編輯部 /
副總編輯 籃貫銘 Korbin Lan
資深編輯 王岫晨 Steven Wang
執行主編 陳復霞 Fuhsia Chen
美術編輯 陳宇宸 Yu Chen
助理編輯 吳雅婷 Tina Wu
特約主筆 王明德 M.D. Wang
特約記者 王景新 Vincent Wang
特約攝影 林鼎皓 Dinghaw Lin

CTIMES 英文網 /
專案經理兼主編 籃貫銘 Korbin Lan
特約編譯 Phil Sweeney

產業服務部 /
經 理 曾善美 Angelia Tseng
主 任 林佳穎 Joanne L. Cheng
主 任 翁家騏 Amy Weng
主 任 曾郁期 Grace Tseng
資深記者 陳念舜 Russell Chen
產服特助 蕭泊皓 Chuck Hsiao

整合行銷部 /
發行專員 孫桂芬 K.F. Sun
張惟婷 Wei Ting Chang

管理資訊部 /
會計主辦 林寶貴 Linda Lin
法務主辦 顏正雄 C.S. Yen
行政專員 張惟婷 Ting Chang

發行人 / 黃俊隆 Robert Huang
發行所 / 遠播資訊股份有限公司
INFOWIN INFORMATION CO., LTD.
地址 / 台北市中山北路三段 29 號 11 樓之 3
電話：（02）2585-5526
傳真：（02）2585-5519

輸出印刷 上海印刷廠股份有限公司
行政院新聞局出版事業登記證
局版北市字第 672 號
中華郵政台北雜字第一四九六號
執照登記為雜誌交寄
國內總經銷 高見文化行銷股份有限公司
（02）2668-9005
港澳總經銷 高業企業股份有限公司
TEL：（852）2409-7246
FAX：（852）2409-6438
紐約總經銷 世界日報 世界書局
洛杉磯總經銷 洛杉磯圖書部
舊金山總經銷 舊金山圖書部
零售商 全台金石堂及各大連鎖書店均售
郵政帳號 16854654
國內零售 180 元
訂閱一年 1800 元
國內掛號 一年加收 250 元掛號費
國外訂閱 普通：港澳 2800
亞太 3150
歐美非 3400

MathWorks®
Accelerating the pace of engineering and science

Are you ready for AI? Is AI ready for you?

MATLAB® & Simulink®

支援模型化基礎設計、各類型資料處理解析等強大功能
之整合式開發平台，協助您做好迎向人工智慧的準備！

模型化基礎設計

- 自動控制設計
- 新一代無線通訊設計
- 軟硬體協同模擬
- 驗證與有效性檢測

C/C++、HDL、CUDA等程式碼自動生成

資料解析

- 資料的取得與探索
- 訊號/影像處理
- 大數據解析
- 機器學習/深度學習，預測模型開發

解析結果與嵌入式硬體、企業系統的整合

業務及技術諮詢
地址：台北市忠孝東路六段21號8樓之3　電話：(02)2788-9300
TeraSoft 鈦思科技
www.terasoft.com.tw
MathWorks®
Accelerating the pace of engineering and science

從2.5D到3D

算算時間，晶片的2.5D製程技術問世至今，已將近10年。如今，3D晶片的製程技術也總算是有了風吹草動，預計在2020年，採用三維堆疊製程的晶片就會正式面市。

而有趣的是，晶片製造商並不把這種三維堆疊製程的晶片稱作3D IC，而是將之命名為「3D封裝（3D Packaging）」技術。由此可知，封裝，才是未來晶片製造的關鍵所在。

從技術上來看，以往認為3D晶片的實踐關鍵在於矽穿孔（TSV）技術，也就是晶圓對晶圓貼合時，用來導引電流進行晶片互連的技術。但演進到目前的實作，TSV的確是關鍵，但僅是其中一項。

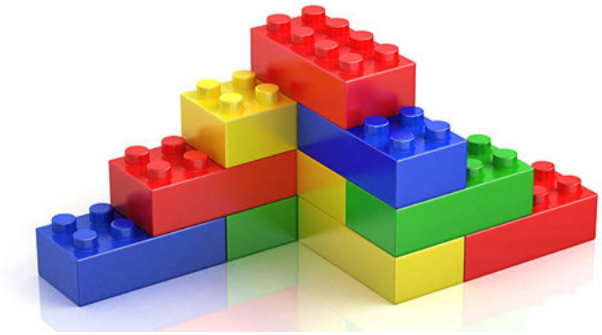
微凸塊/微焊球（μ-bumps）的技術也很重要，它直接關係到電傳效率與性能；而最後把這些成疊、成塊的微晶片（chiplet）一起打包的技術更是重要，一顆晶片最後能不能用，就看這一步了。

所以，TSV只是起了個頭，最終要實現3D IC的製造，是要仰賴一系列複雜又精密的流程，而它關係到更多是在封裝領域的著墨，也因此主要的晶片製造商都紛紛投入此技術的研發。

效能提升當然是新一代封裝技術的亮點，但對企業經營來說，效能只是其中一個優勢，成本則是另一個。所以如何透過降成本的方式，來讓新一代封裝技術可以更快進入市場，也是值得思考的方法。面板級扇出封裝（FOPLP）就是在這樣的思考下產生的。只談技術不談營收，往往是不切實際的。

另一種封裝思考，是異質整合，就是把以前沒結合過的東西，試著結合在一起。在目前IoT與5G時代裡，最有趣的是，就是封裝天線的技術「AiP」，也是發展另一種維度的思考。

所以整個來看，3D晶片其實並不只是一種製程技術，反而更接近一種設計思考，如何從有限的2D和2.5D架構中，跳脫出來，讓更多的功能與應用可以被整合進來。而有3D設計的思維之後，4D的時代也就不遠了。



副總編輯

CTIMES 編輯大綱

2019 CONTENT PLAN

01 JAN

封面故事：2019產業回顧與展望

專題報導：8-bit MCU
量測專欄：5G量測

關鍵技術報告：AI

02 FEB

封面故事：人工神經網路：ANN

專題報導：感測技術
量測專欄：示波器

關鍵技術報告：感測器

03 MAR

封面故事：廢電子回收技術

專題報導：電源管理
量測專欄：信號產生器

關鍵技術報告：LPWAN

04 APR

封面故事：C-V2X

專題報導：NB-IoT
量測專欄：IoT量測

關鍵技術報告：車用電子

05 MAY

封面故事：USB PD

專題報導：SerDes技術
量測專欄：高速數位量測

關鍵技術報告：IoT

06 JUN

封面故事：SSD & HDD

專題報導：BMS電池管理
量測專欄：網路分析儀

關鍵技術報告：MCU

07 JUL

封面故事：次世代封裝

專題報導：COMPUTEX展後報導
量測專欄：邏輯分析儀

關鍵技術報告：嵌入式設計

08 AUG

封面故事：人機協作

專題報導：工業感測器
量測專欄：混合訊號示波器

關鍵技術報告：工業控制IC

09 SEP

封面故事：EDA

專題報導：PCB設計
量測專欄：毫米波量測

關鍵技術報告：Micro LED控制

10 OCT

封面故事：人工神經網路：異質整合

專題報導：MRAM, FRAM
量測專欄：半導體測試

關鍵技術報告：無線通訊

11 NOV

封面故事：區塊鏈

專題報導：邊緣運算
量測專欄：模組化儀器

關鍵技術報告：電源控制

12 DEC

封面故事：年度產業調查

專題報導：軟性顯示
量測專欄：無線通訊量測

關鍵技術報告：能源與電池

洪春暉
資策會產業情報研究所(MIC)
副所長

資料轉化價值形成企業新競爭優劣之契機

如何促進資料持有者願意提供高品質的資料，是各國在推動資料交易市場優先要面對的課題。

在數位化及萬物聯網的時代，AI、區塊鏈、機器人等技術變革帶動資料量呈指數成長，也提高了我們處理大量資料的能力，有機會將資料轉化為具重大社會經濟價值的產品，而這一變化，為我們的經濟和社會提供進一步成長與改變的契機。對企業來說，運用資料轉化為可操作且有價值的洞見與決策，也構成了一種新的競爭優勢，提供企業加速茁壯成長的機會。

然而，有效的資料蒐集並不是每個企業都有能力去做，且資料的價值需要有資料提供為前提，透過資料的聚合和有效使用才會顯現，這也是發展資料交易服務市場的本質，以滿足資料使用者可以依據需求購買所需的資料。

因此，如何促進資料持有者願意提供高品質的資料，是各國在推動資料交易市場優先要面對的課題。例如新加坡建立一個整合公部門和私人企業資料的資料市集平台，以解決資料提供者和資料使用者面臨的障礙。該平台旨在協助資料持有者透過資料授權將資料貨幣化而實現收益，希望促進更多的參與者加入，形成活躍的資料共享生態系。

GDPR改變個人資料所有權的遊戲

近來，除了個人資料可以由第三方機構蒐集、處理與共享的方式，引發公眾討論和關注之外，2018年歐盟GDPR（General Data Protection Regulation)正式上路、英國新資料保護法 (The Data Protection Act)的推出，提供個人有關其資料使用方式，如同意、可攜性及刪除等強大權利，開始改變消費者對資料的看法，推動個人資料經濟的發展。換言之，個人擁有自己的資料，然後可以選擇與信任的第三方共享，並從共享中獲利。

讓個人持有自己的資料，對個人和企業都有好處。首先，由於資料是儲存在個人端，駭客無法一次竊取龐大資料量，資料安全性相對提高。再者，多數人通常不會隨時去更新自己的線上帳戶資料，但當個人保有自己的記錄時，資料正確性問題便可獲得解決。而對企業來說，當消費者擁有個人資料時，大型資料集的建置需求減少，因此可降低企業的資料管理成本，以及解決監管問題。

其實大多數人是願意交換他們的資料來獲得有用和可信賴的服務。然而，在制度和系統還不完備的情況下，有些人擔心他們共享的資料是否在未經他們同意下傳送，以及是否會被盜。因此，提供創新企業開發服務的機會點。

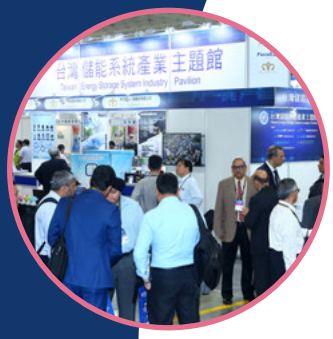
（本文由資策會MIC洪春暉、勵秀玲共同執筆）

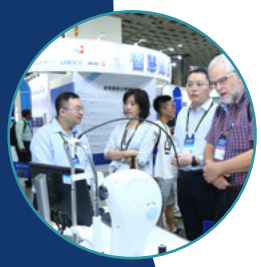
TAITRONICS
台北國際電子產業科技展

AIoT Taiwan
台灣國際人工智慧暨物聯網展

2019年10月16 - 18日

台北南港展覽館1館 (TaiNEX 1)





TAITRONICS
台北國際電子產業科技展

臺灣為全球電子產業供應大國，根據台灣區電機電子工業同業公會統計，2018年我國資通訊及電機電子業出口額達新臺幣4.87兆元，較2017年出口額增3.5%，占我國全年出口總額逾3成；受到智慧型手機銷售量下滑影響，市場預估2019年各項電子終端產品出貨成長都將放緩，惟雲端服務業務持續發展，對我國晶圓代工和伺服器產品需求仍會延續。工研院IEK預測，2019年資訊電子業產值可望達為新臺幣6.67兆元，年增2.2%，可見臺灣持續於講求高度精密與不斷創新的電子產業當中掌握優勢。2019年電子展將整合專業展區，引領廠商掌握商機、接軌國際！

TAITRONICS展區:

- 電子零組件及配件
- 儀表儀器
- 電機及自動化設備
- 電池與電源供應器
- LED照明與應用

www.taitronics.tw

AIoT Taiwan
台灣國際人工智慧暨物聯網展

臺灣在扮演世界電子製造樞紐的同時，隨著5G商轉、大數據分析、專用運算晶片及超級電腦高速處理時代的到來，人工智慧(AI)生態系應用不斷擴大，透過與物聯網(IoT)網絡連結，逐漸匯流為AIoT，使驅動智慧應用大放異彩。臺灣擁有世界一流的人才，搭載全球頂尖的硬體製造水準，2019年吸引亞馬遜雲端運算(AWS)在臺灣設置大中華區首座IoT Lab。掌握科技革新，從需求出發、定義新興產業鏈、推動系統與服務的成果，2019年「台灣國際人工智慧暨物聯網展」將聚焦AIoT應用及解決方案，並首度設置「新創」專區，展現臺灣產業在物聯網時代的轉型與創新實力。

AIoT Taiwan展區:

- 智慧製造
- 智慧商業
- 智慧照護
- 智慧居家
- 智慧校園
- 新創展區
- 智慧農業及食安
- 雲端及寬頻通訊

www.aiottaiwan.com

主辦：中華民國對外貿易發展協會 台灣區電機電子工業同業公會

亭心觀測站

一個地球 自在悠遊

文/亭心

工業革命或稱產業革命以來，地球資源遭到人類過度開發，森林消失、河流乾涸、空氣汙染、物種滅絕，一條條公路取代了幽徑渠道，一個個裝置取代了蟲鳴鳥叫，雖然人們的控制領域擴大了，但是束縛似乎卻更多了。或許有人認為這是科技的問題，當然不是，科技只是使速度加快而已，問題的根本在人類的愚昧貪婪。懂得用火、懂得用刀時，問題就不比現在輕鬆，看看白起在長平之戰用巧計殺死趙軍40萬人就知道，這是火與刀科技所造成的嗎？

解決科技被濫用的問題還是得靠科技，這是自然的因果律，就好像從哪裡跌倒就得從哪裡爬起來的道理一樣。雖然地球上不公平的資源與不對稱的力量一直存在，但科技應該以打造公平與對稱的環境而努力，既然地球表面已被濫墾、濫用殆盡，再在地表上疊床架屋就顯得非常不智，不如讓地表休養生息一下，往太空或次太空建設發展就是一條路。

6月25日台美共同合作執行的「福衛七號」氣象衛星群成功發射，並且在173分鐘後接收到全部6顆衛星的訊號。除了發射技術之外，在數位科技背景下衛星的發展，一樣可以越來越輕薄短小，且功能越來越強大多樣，所以台灣的創意與技術當然可以發展這樣的新產業，也為國際社會貢獻一份心力。值得一提的是福衛七號也是委由SpaceX公司發展的火箭所搭載發射，這家公司早就看到了太空領域的潛力，一連串的事業理想也正在進行中。

地球上目前最不平等的現象就是數位資源分配與資訊不對稱的問題，估計全球70多億人口中仍有約30億人沒有或無法使用網際網路（至2018年底全球約54.4%的人有使用網際網路(註一)）。另外使用網際網路的人口中也不是都通暢無阻，中國建構的防火牆，使14億中國人的資訊取得受到嚴格控管，至於身處高山、大海或空中的人，也不在網路通訊可覆蓋的範圍；所以不論是人為或自然因素所造成的障礙，都可以說是一種數位藩籬（digital divide），有藩籬就有剝削，就是科技發展的災難。

進入太空科技可以舒緩這個問題嗎？是的，這是解決目前數位藩籬的突破點，有識之士SpaceX公司的創辦人馬斯克（Elon Musk）也意識到了這一點，於是在2015年提出了所謂的「星鏈計劃（Starlink）(註二)」，預計2020年前在太空中部署11943顆通信衛星。此一衛星群建成之後，將具有全覆蓋、高通量與低延遲的特點，等於提供全球各地人口一個低價、高速、無死角的WiFi上網服務。這個計劃乍聽之下有點誇張，目前最大的衛星群也只有65顆，但在今年5月24日SpaceX一次發射部署了60顆衛星後，質疑的聲音也就越來越少了。

星鏈計劃完成會是一個什麼樣的世界？最重要當然就是數位藩籬的打破，這一點雖然不須要用理想完美的方式來看待，但對於各個層面的影響實在非常深遠，未來無論是政治、經濟、科技或法律層面，都將面臨考驗。可能國家的界線或定義會被打破，住居與交通的觀念會被打破，生產與消費的觀念也會被打破，大家不妨跟著想像一下，馬斯克創辦的PayPal、特斯拉與SpaceX這三家公司，不就都是這樣突破實現的嗎？

期待有一天，在星鏈之類數位通信衛星的導引下，地球面貌改變了，不再有交錯的公路網、不再有城市與偏鄉之分、不再有莫名的生產與浪費，而是全家大小駕著低空飛行器，遨遊在地球的每一個角落。■

地球表面已被濫墾、濫用殆盡，再在地表上疊床架屋就顯得非常不智，不如讓地表休養生息一下，往太空或次太空建設發展就是一條路。(註三)

註一：https://zh.wikipedia.org/wiki/全球網際網路使用率

註二：七分鐘了解星鏈計劃：https://www.youtube.com/watch?v=lb_T5PNmby8

註三：福衛七號與獵鷹火箭發射前英姿（SpaceX）

作者：顏睿余
Microchip 應用工程師

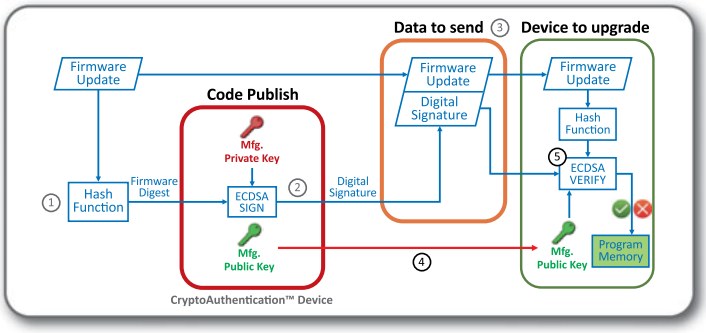
非對稱式 Security Boot/Security Update 的實作

小百科

Security Boot 是一種用於確保系統內運作的應用程式碼被授權的方法，通常由設計與構建系統的廠商提供。通過確保應用程式碼為正確的授權版本可以防止不可預測的系統程式造成機器性能異常、安全性受損甚至財產損失。大多數電子系統使用可編程非揮發性存儲器 (Flash) 存放其應用程式碼 (Application Code)，無論大小都可以利用 Security Boot 保護該程式碼不被惡意竄改。本文說明 Security Boot 的基本觀念，同時深入地介紹其處理方式並提供解決方案。

Security Update 流程

前置作業：下圖紅色方框所代表的角色為程式碼簽發者 (Code Publish)，其包含一組唯一的公鑰 (Public Key) 和私鑰 (Private Key)



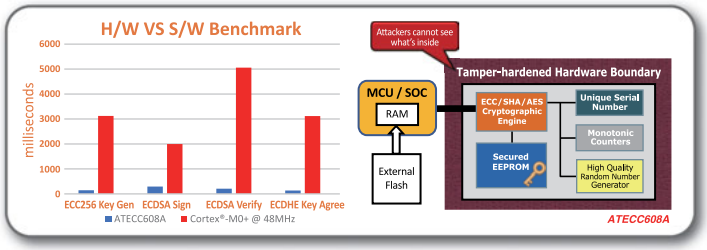
1. 要進行升級的應用程式 (Firmware update) 應該要先透過 Hash Function (例如 SHA256) 獲取其 Digest (此步驟就如同用 XOR 計算出程式碼的 Checksum，只是 SHA256 Digest 為 256-bit 遠大於 Checksum，具有絕對唯一性)。
2. 接著程式碼的簽發機構 (Code Publish) 需要針對該程式碼的 Digest 透過其私鑰進行“加密”(ECDSA SIGN)，加密過後的資料我們稱作數位簽章 (Digital Signature)。因為擁有該私鑰即擁有權力簽發正式版本程式碼的數位簽章，故一般而言私鑰將會被存放於硬體保護的晶片裡 (如 ATECC608A)，避免對外流傳。
3. 將更新應用程式與數位簽章 (Data to Send) 透過有線或是無線的方式傳送至待更新的裝置 (Device to Upgrade)。進行更新之前，待更新裝置必須驗證此應用程式與數位簽章的正確性。
4. 在非對稱的算法中，每個存在的私鑰會有一個相對的公鑰存在，其私鑰用來“加密”(ECDSA SIGN)，公鑰則用來“解密”(ECDSA VERIFY)，故更新裝置中應該要預先配備相對的公鑰。為了能限制僅搭配特定的程式碼簽發機構 (Code Publish) 作“解密”，其公鑰必須存放在一次性燒錄的記憶體中 (OTP)，避免被更換為駭客私鑰的對應公鑰。
5. 更新裝置 (Device to Upgrade) 在收到更新程式 (Firmware update) 後即先透過 Hash function (例如 SHA256) 獲取其 Digest (如同第 1 步驟)，為確認該 Digest 是否正確，必須透過公鑰對同步收到的數位簽章作解密並判斷是否符合更新程式的 Digest (ECDSA VERIFY)。若是符合，則該更新程式允以更新該裝置。反之，假設該更新程式並非官方發行程式碼 (沒有透過 Code Publish 簽發數位簽章)，經過第 5 步驟的驗證，因為其計算出來的 Digest 將不同於透過公鑰所解密的數位簽章，該程式碼則不予運作。

Security Boot 流程

如同 Security Update 流程第 5 步驟，開機後即先透過 Hash Function (例如 SHA256) 計算應用程式之 Digest，接著確認該 Digest 是否正確：透過公鑰對數位簽章作解密並判斷是否符合該應用程式的 Digest (ECDSA VERIFY)。

運行 Security Update 之裝置需求

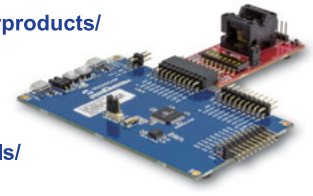
1. **一次性燒錄的記憶體**
   為了能夠完成 Security Update/Security Boot 流程，其中步驟 4 提到裝置必須預先配備公鑰於一次性燒錄的記憶體中 (OTP)，目前市售 MCU 提供 OTP 功能的並不多，或者價錢相對不便宜。
2. **進行 ECDSA VERIFY 運算**
   步驟 5 中提到需要對應用程式 Digest 與程式碼數位簽章利用 OTP 區的公鑰進行 ECDSA VERIFY 運算。該運算量相當龐大，如下圖若以 Cortex®-M0+ 進行運算將耗費 5 秒。開機若需要耗費如此多的時間將不容易被使用者接受。



Microchip 提供 ATECC608A 可外掛支援 Security Boot 功能

ATECC608A 提供基於硬體的密鑰儲存與加密算法加速器，用以實現各種身分驗證和加密協議，基於落實 Security Boot。使用者能預先將公鑰存放於 ATECC608A 的 Secured EEPROM 中，並透過 ECDSA 硬體加速器進行 Digest 和數位簽章的驗證運算 (Verify)。而運算結果亦可以透過輸出保護密鑰 (IO Protection Key) 輸出，駭客無法判讀或進行複製。相關產品資訊請參考官方網站：

- **ATECC608A 產品頁面**
  https://www.microchip.com/wwwproducts/en/atecc608a
- **ATECC608A 開發工具**
  https://www.microchip.com/DevelopmentTools/ProductDetails/DM320109



聯繫信息 > Microchip 台灣分公司
電郵：rtc.taipei@microchip.com　　技術支援專線：0800-717-718
聯絡電話：• 新竹 (03) 577-8366　• 高雄 (07) 213-7830　• 台北 (02) 2508-8600

衛福七號升空 點亮台灣的太空產業供應鏈

從整體價格，以及目前的研發、製造與發射流程來看，探索太空已經從國家等級，變成企業等級的營運範圍，因此必然也將形成所謂的「太空產業」。

在國人的期待與掌聲中，福爾摩沙衛星七號（福衛七號）在美國太空探索公司（SpaceX）獵鷹重型火箭（Falcon Heavy）的載送下，順利於美國甘迺迪太空中心發射升空。而這次的成功發射，再次顯示了太空產業已不再遙不可及，而且還將會越來越親民。

這次的發射有幾個重點，首先當然是福衛七號，它是繼2006年福衛三號升空之後，另一次台灣與美國共同合作開發的衛星，其中有不少的元件與系統，都是由台灣自主研發設計的（福衛五號則是首個台灣自製的衛星）。

特別是其中的獵風者衛星（Triton）完全由台灣自行研發，包含GNSS-Reflectometry酬載、衛星電腦、電力控制單元、GPS接收機、光纖陀螺儀與過氧化氫衛星推進模組等。

再者，則是造價進一步降低，福衛七號的台灣造價僅約32億台幣。相對於2017年8月發射的福衛五號，總經費達新台幣56.59億元，又進一步縮減。

另一個重點則是SpaceX的獵鷹重型火箭（Falcon Heavy），雖然此次主推進器的回收失敗，但它還是目前最經濟的太空發射器。而且隨著經驗與技術的持續成熟，預料價格還可以進一步降低。

從這次包含福衛七號在內，共運送了24顆的衛星來看，Falcon Heavy的運送價格想必是有一定的吸引力，才能夠吸引這麼多的客戶響應。

所以從整體的價格，以及目前的研發、製造與發射流程來看，探索太空已經從國家等級，變成企業等級的營運範圍，因此必然也將形成所謂的「太空產業」。

目前行政院也已經核定了台灣的太空科技長程發展計畫，將花費十年的時間，從2019年起至2028年，投入251億元，結合產學界能量，自主開發十顆衛星，藉此發展商用元件及通用型衛星本體平台，並自行發展關鍵零組件，帶動台灣太空產業發展。

除了學界的投入，台灣的產業界則包括久鴻國際、中華電信、公準精密、宏誠動力、金頓科技、芳興科技、晉陞太空科技、凌群電腦、得安科技、莘茂複材、捷揚航電、創未來科技、創宇航太、微像科技、達雲科技、經緯航太、廣碩系統、鴻緯科技、寶瀛科技、漢翔等，也都已經投入台灣的太空科技發展計畫。(籃貫銘)

SEMI：全球晶圓廠設備支出將於2020年回彈20%

SEMI（國際半導體產業協會）更新了2019年第二季全球晶圓廠預測報告（World Fab Forecast），指出全球晶圓廠設備支出繼2019年下滑19%至484億美元之後，2020年將成長20%，達584億美元。第二季的更新下修了今年稍早對2020年預估27%的成長率，2019年的支出也由原先的下滑14%，進一步降低至19%。儘管2020年預料將有所反彈，晶圓廠支出仍將較2018年的投資金額少20億美元。

根據預估，今年單是記憶體產業的支出將下滑45%，占2019年降幅的絕大部分，但2020年可望強勁復甦45%，達280億美元。2020年記憶體相關投資將比前一年增成長超過80億美元，並帶動晶圓廠支出的復甦，然而與2017、2018年相比，2020年記憶體相關投資仍將遠低於先前水準。儘管今年記憶體產業支出大幅縮減，但晶圓代工產業相關和微處理器晶片（micro）產業的投資可望逆勢成長。