

# Andes e-Report

- 晶心科技與合作開發工具供應商攜手為AndesCore™ V5 N25及NX25處理器推出先進SoC開發環境.....P.1
- 晶心科技推出超純量(Superscalar)系列處理器N15(F)、D15(F).....P.4
- 晶心處理器證實無Meltdown和Spectre安全漏洞.....P.5
- 晶心科技、SecureRF攜手推出抵禦量子攻擊的安全解決方案 瞄準資源有限物聯網裝置 提供高效率、低功耗的驗證及資料保護解決方案.....P.6



## 晶心科技與合作開發工具 供應商攜手為AndesCore™ V5 N25及NX25處理器 推出先進SoC開發環境

晶心科技(TWSE：6533)，低功耗、高效能之32/64位元嵌入式CPU IP(Intellectual Property)亞洲領導供應商及RISC-V基金會創始會員，宣布與合作夥伴Imperas、Lauterbach、西門子子公司Mentor以及UltraSoC(依字母順序排序)等世界級開發工具及IP供應商共同合作，推出適合晶心V5處理器及RISC-V社群之SoC的開發工具環境。

晶心科技在CPU IP領域耕耘超過12年，採用晶心指令集架構的SoC應用領域非常多元，全球累計出貨量已超過24億顆。與時俱進的晶心科技，為RISC-V社群新推出採用以RISC-V架構為子集的第五代AndeStar™ V5指令集。而以V5為基礎的32位元N25與64位元NX25 AndesCore™處理器皆為高性能，操作頻率可超過1 GHz(在台積電28奈米HPC製程下)，提供不低於2.8 DMIPS/MHz與3.4 CoreMark/MHz的優異性能，而邏輯閘數更可分別低至30K及50K。因此N25及NX25非常適合網路、儲存及人工智慧(AI)等需高速控制的各種應用。

「為了支援功能不斷增加的新興應用，SoC工程師面臨設計複雜性和上市時間(time-to-market)的挑戰，因此需要強大的開發工具，如用於架構探索與軟體開發的快速系統模擬、功能與系統驗證的仿真(emulation)、性能最佳化、錯誤追蹤及嵌入分析等等，這也是晶心科技已與V3 AndesCore™處理器的夥伴合作多年的重要原因，」晶心科技總經理林志明強調，「現在我們正攜手Imperas、Lauterbach、Mentor及UltraSoC，繼續為晶心科技的新V5 AndesCore™ N25及NX25提供先進系統開發工具環境。我們很高興能藉合作夥伴的大力支援讓RISC-V生態系更加豐富，並期待未來很快能見到共同客戶充滿創意的產品誕生。」

「Imperas的Open Virtual Platforms (OVP) Fast Processor Models支援晶心科技AndeStar™ V5處理器，並以基於虛擬平台的工具協助開發、移植、除錯和測試在V5處理器上所運行的軟體和作業系統。Imperas很高興能與Andes合作，為新興RISC-V生態系提供新一代模型、Extendable Platform Kits (EPKs)及軟體開發解決方案，以加速其應用。」Imperas執行長Simon Davidmann表示。

Lauterbach國際業務及行銷經理暨行銷主管Norbert Weiss說：「Lauterbach TRACE32支援AndeStar™ V3架構和核心多年，很高興能繼續支援新一代具增強擴充架構的RISC-V N25及 NX25處理器，讓使用晶心科技新V5處理器開發產品的工程師，能有效利用TRACE32進行完整除錯功能，包括bootstrap程式碼、interrupt routines(中斷程式)及驅動程式。」

Mentor仿真部門副總裁暨總經理Eric Selosse表示：「Mentor與晶心科技的合作，能確保我們的共同客戶獲得完美搭配N25及NX25 AndesCore™處理器IP仿真平台的最佳支援。我們的Veloce®仿真平台支援V5處理器，協助建立精簡且連貫SoC的設計及開發程序。」

UltraSoC執行長Rupert Baines指出：「UltraSoC承諾對於晶心科技V5處理器的支持，藉由合作夥伴與UltraSoC RISC-V基金會會員的身分，共同積極推動業界採用RISC-V。透過晶心科技的V5處理器以及UltraSoC的on-chip追蹤及除錯IP讓晶片製造商能利用開源硬體的優勢推出更多創新設計。」

身為第一個採用RISC-V指令集架構的主流CPU IP供應商，晶心科技自從加入RISC-V基金會以來，一直積極貢獻GNU和LLVM等開源工具鏈，並與合作夥伴致力於擴大RISC-V的生態系。晶心科技根據12年來與客戶互動所獲得的回饋意見，推出了快

速、小型並具豐富擴充功能的五級管線V5 N25和NX25處理器。晶心科技承諾與合作夥伴積極加速推動業界接受RISC-V。

### 關於Imperas

Imperas提供的方案、技術和產品，有助提升嵌入式系統開發、除錯和軟體測試的效率。Imperas的用戶來自處理器IP市場、半導體供應商和嵌入式系統業者，他們對於軟體品質和可靠性以及功能安全性與安防有高度要求。基於Imperas虛擬平台的產品使用Open Virtual Platforms (OVP)模型和API，支援包括RISC-V核心等超過180種的處理器核心。

### 關於Lauterbach

Lauterbach是一家完整、模組化和可升級的微處理器開發工具全球領導製造商，自1979年成立至今，在嵌入式設計領域擁有豐富經驗。Lauterbach在全球各地擁有許多大型客戶，並與半導體廠緊密合作，是一家信譽卓著的國際公司。該公司工程團隊開發生產高品質和專業化的TRACE32®系列開發工具。

### 關於Mentor Graphics

西門子子公司Mentor Graphics是全球電子硬體和軟體設計解決方案的領導者，為全球電子、半導體和系統等領導業者提供產品、諮詢服務和獲獎項肯定的支援服務。

### 關於UltraSoC

UltraSoC為複雜SoC提供除錯(運行控制、追蹤等等)之半導體IP，協助開發、優化、除錯及降低功耗與成本，可用於pre-silicon階段來加速仿真和打造原型，或於post-silicon階段來支援軟硬體整合甚至到實地使用場景(in-field/in-use)。UltraSoC完整支援RISC-V(及其他CPUs，如異質多核心)；其除錯範圍不僅限於CPU，還包含整個SoC。

# 晶心科技推出超純量(Superscalar)系列處理器

## N15(F)、D15(F)

亞洲首家以原創性32/64位元處理器IP與系統晶片設計平台為主要產品的晶心科技(Andes Technology, TWSE: 6533), 推出一系列基於AndeStar™ V3架構、高效率的超純量(Superscalar)處理器 AndeCore™ N15/N15F/D15/D15F。其中N15採用基礎(Baseline)指令集, D15為N15加上數位信號處理(DSP)延伸指令集功能, 而N15F與D15F分別是N15跟D15加上浮點運算單元(Floating Point Unit)。此一系列產品可應用在傳感器設備、智能儀表、生物識別、通信領域、音頻、語音、圖像處理、醫療器械、工業、無人機和汽車全球定位系統(GPS)、無人機、降噪(Noise reduction)及回音消除(Echo cancellation)等領域。

N15(F)、D15(F)是具有雙發射管線(Dual-issue pipeline)的處理器, 提供同級產品中最高5.41 CoreMark/MHz效能。工作頻率方面, 於40LP製程下可達500MHz並提供各種可配置選項, 包括: 可支援Linux作業系統的記憶體管理單元(MMU)、可應用在使用者存取區域資料控制的記憶體保護單元(MPU); 指令及資料的快取記憶體(Cache)及區域記憶體(Local memory)的大小, 分別可支援到64KB及16MB, 並且均具有錯誤更正碼(ECC)的功能選項有助於提升整體SoC的穩定度; 內建符合IEEE-754標準規格支援單精度(Single-precision)及雙精度(Double-precision)的浮點運算單元(Floating Point Unit); 數位信號處理(DSP)延伸指令集, 定義了超過130個DSP及SIMD指令, 於配合C/C++編譯器支援及超過200個優化的DSP程式庫時, 可使應用數位訊號處理的程式開發更容易、更有效率。除此之外, 64位元資料寬度的快取記憶體、區域記憶體及匯流排, 可增加指令(Instruction)讀取和數據(Data)存取的頻寬, 進一步提升效能。這個系列的產品適用於嵌入式Linux、即時作業系統(Real-time OS)或無作業系統等多種不同效能需求的應用環境。

D15(F)系列的DSP指令, 不僅具備包含飽和(Saturation)運算的一般常用DSP指令, 還內建8位元及16位元的SIMD指令, 可在單一時脈同時處理4個8位元或2個16位元的資料, 大幅提升矩陣運算、濾波器、傅立葉轉換及統計方面的執行效能。另外, D15(F)系列也支援64位元的加減法及與乘法混合的運算, 提供支援ZOL (Zero Overhead Loop)指令來消除迴圈分支的負擔, 提高效率, 以因應講求效能的各類多媒體應用需求。

晶心科技技術長兼資深研發副總經理蘇泓萌博士表示，D15(F)/N15(F)系列是基於6級非對稱式(Asymmetrical)雙發射管線架構設計的全方位處理器，兩條管線分別處理不同功能的指令。這種非對稱性的架構使用較少的硬體資源及更低的功耗，但在編譯器絕佳配合之下卻可達領先業界的效能。其中的乘法可在一個時脈完成32x32的運算或兩個16x16的運算。除法採用Radix-4的除法，比傳統的除法器最多可快14個時脈週期。另外，除了數位信號處理延伸指令集及浮點運算指令外，N15(F)/D15(F)並提供增進處理器效能的動態分支預測(Dynamic Branch Predication)及高效率的64位元AXI4 bus。在除錯方面，除了支援傳統的方式，還支援進階的追蹤(Trace)模式，可將一段程式執行的過程記錄下來，讓除錯更有效率。

與業界同級的超純量產品相比，N15(F)/D15(F)的3.36 DMIPS/MHz效能高32%；於28HPM製程下，面積少20%、功耗省45%；在DSP主要應用功能的比較，在平均效能方面超出97%；而浮點運算單元的基準測試則有高於48%的表現。

總而言之，N15(F)/D15(F)整合優越的超純量硬體架構效能及內建的浮點運算單元，最佳化的編譯器及高效能的DSP程式庫，能充分滿足各種應用的需求，協助客戶縮短開發時間，輕鬆研發出具有競爭力的產品。D15F目前已授權給客戶用來設計多媒體晶片。

## 晶心處理器證實無Meltdown和Spectre安全漏洞

近期關於橫跨多個指令集架構的兩個處理器安全漏洞的大量新聞報導，引發全球高度關注處理器系統的安全議題。晶心科技擁有多多年嵌入式處理器開發經驗，並致力於確保晶心處理器嵌入式系統的安全。經全面查核，晶心科技特別發表聲明，確認晶心處理器安全無虞，並未受Meltdown和Spectre影響。

「安全性對進行SoC設計的晶心客戶來說十分重要，我們一直密切關注這兩個利用推測執行竊取機敏資料的Meltdown及Spectre攻擊。」晶心科技技術長兼資深研發副總經理蘇泓萌博士表示，「經過詳細分析，我們確認AndesCore™處理器的管線設計不會受到攻擊。當遇到違反權限的事件時，我們的處理器不會執行後續的存取；而我們的分支推測深度不至於讓隨後的指令可以產生旁通道(side-channel)的資訊外洩。此外，我們的AndesCore S8處理器更具備強大防護能力，不僅能抵禦像Meltdown及

Spectre等攻擊對未授權資料的存取，而且面臨高能輻射等實體攻擊時也能避免資訊外洩。」

「正當全球關注這起事件的發展，晶心科技主動進行自我查核並公布結果，確保客戶產品的安全。由於並無任何晶心處理器受Meltdown或Spectre的缺陷影響，嵌入晶心處理器的SoC若已進入市場，也無須採取緩解因應措施。」晶心科技總經理林志明表示，「不過，為了強化AndesCore處理器的安全，晶心科技仍將密切追蹤處理器安全議題的最新分析及消息，以作為未來設計處理器的參考。」

晶心處理器產品包括N、D、E、S及NX系列的AndesCore處理器。雖然其中S系列處理器是主打安全防護功能的產品，不過晶心科技也了解AndesCore的其他系列處理器的應用也有機會在有安全風險的開放環境中處理機敏資訊。隨著處理器硬體的安全性越來越受重視，晶心科技會持續不斷的加強全系列處理器的安全防護功能。

## 晶心科技、SecureRF攜手 推出抵禦量子攻擊的安全解決方案

瞄準資源有限物聯網裝置  
提供高效率、低功耗的驗證及資料保護解決方案

自主研發小面積、低功耗、高效能之32/64位元嵌入式處理器核心IP (Intellectual Property)的亞洲領導供應商晶心科技(TWSE: 6533)及位於美國康乃狄克州謝爾頓市的抵禦量子電腦攻擊(quantum-resistant)物聯網(IoT)安全解決方案領導供應商SecureRF，宣布結合AndesCore™安全處理器IP和SecureRF的非對稱式(公鑰)加密，共同為資源有限的物聯網裝置提供快速且高效率的量子安全防禦。晶心科技的安全記憶體保護及防竄改防護技術，能抵禦駭客攻擊；而SecureRF的驗證及資料保護解決方案則為輕巧、精簡且要求極低功耗的物聯網裝置提供更強大的保護。

由於大部分安全解決方案須大量耗費記憶體及電力，缺少資源之32/16/8位元物聯網裝置往往僅有低度保護或甚至無任何保護。此外，許多安全解決方案需要網路連線及管理通用鑰匙或密碼資料庫，然而這些資料庫往往也有安全風險，尤其經由大量工業級和消費級產品銷往全球各地的情況下，其管控更加不易。SecureRF的非對稱式解決方案，包括Ironwood™ Key Agreement Protocol 及Walnut Digital Signature

Algorithm (WalnutDSA™)，提供強大且快速的安全防護，即使未來量子電腦時代來臨，也能有效保護物聯網裝置。SecureRF的加密協定是基於Group Theoretic Cryptography演算法，較ECC技術快60倍，最低功耗則僅其140分之1，而且無須管理資料庫或維持網路連線。

晶心科技的32位元AndesCore™ S801安全處理器IP能完美搭配SecureRF的安全解決方案。S801採安全記憶體保護單元(SMPU)，可根據安全等級隔離且保護不同用戶及應用。S801亦提供獨特防竄改保護，抵禦實體故障注入(fault injection)攻擊及側通道(side channel)攻擊，其指令/資料/位置攪亂(scrambling)、安全中斷及安全除錯功能可有效防止針對CPU介面的駭客攻擊。

晶心科技總經理林志明表示：「可於受限環境下以高效率運行、高效能驗證和資料安全保護解決方案的需求正在高速成長。與SecureRF合作讓我們能瞄準此需求，提供易於運用的高性價比矽智財(IP)解決方案，協助智慧卡、智慧家電、穿戴式裝置及其他資源有限之物聯網應用開發的企業能完整保護其用戶。」

SecureRF執行長Louis Parks表示：「除非物聯網裝置普遍具備安全驗證和資料保護功能，否則將難以廣為消費者接受。藉由結合我們的可抵禦量子攻擊加密系統與AndesCore™處理器IP，物聯網裝置製造商得以確保客戶的資料及裝置存取受到完整保護，並取得競爭優勢。」

### 關於SecureRF

SecureRF (securerf.com)針對資源有限的物聯網用處理器開發並授權抵禦量子攻擊公鑰安全防護工具。相較於ECC及RSA等技術，SecureRF提供的驗證及資料保護解決方案具備更高效能，其超低功耗、高效率且佔用極小晶片面積 (small footprint)的解決方案，適合32、16、甚至8位元裝置。

SecureRF提供的安全防護解決方案，除了瞄準無線感測器、NFC、藍牙、RFID標籤，也包括FPGA、微控制器及ASIC等嵌入式平台。軟體開發套件、RTL及工具適用於各種不同環境。該公司亦提供Veridify®完整雲端解決方案，透過智慧應用程式提供即時連線，讓產品及供應鏈更智慧、安全、透明。