從原型到商用　自動駕駛技術挑戰多

* 2019年11月28日
* 顧正書，EETC

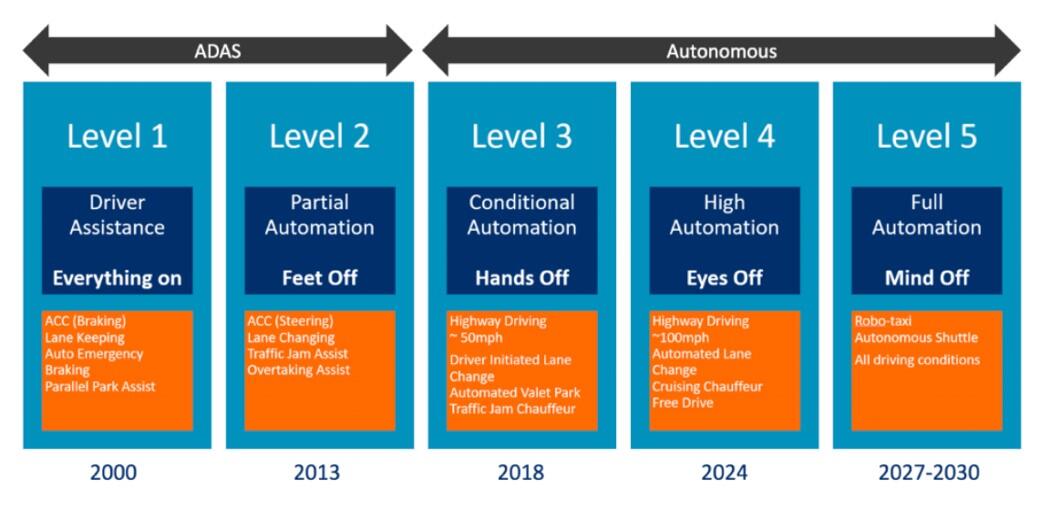
雖然近年自動駕駛吸引了企業、政府、媒體和消費者的普遍關注，但自動駕駛目前仍處於原型測試驗證階段…究竟，自動駕駛從原型到商用化，將面臨那些挑戰？

雖然近年自動駕駛吸引了企業、政府、媒體和消費者的普遍關注，但自動駕駛目前仍處於原型測試驗證階段。多家公司都在路測自己的自動駕駛車輛，包括Waymo、特斯拉(Tesla)、Uber、百度、滴滴，以及傳統汽車OEM如通用(GM)、福特(Ford)、豐田(Toyota)和福斯(Volkswagen)等；自動駕駛晶片和系統方案供應商包括Nvidia、英特爾Mobileye、地平線、NXP等。

Waymo源自Google的一個自動駕駛研究專案，現已成為Google母公司Alphabet旗下的一個獨立公司。截至2018年10月，Waymo自動駕駛車輛已經在美國6個州的25個城市完成公共道路測試里程1,000萬英哩，其虛擬自動駕駛車輛完成了70億英哩的模擬路測。2018年12月，該公司在美國亞利桑那州太陽城正式推出Level 4等級的自動駕駛計程車服務；今年7月，Waymo獲得加州政府頒發的載運乘客服務許可，將在Google總部附近的幾個城市提供無人駕駛出租服務。

從ADAS到全自動駕駛

Waymo自動駕駛研發和路測歷時10年，耗資超過10億美元，目前已經達到Level 4，這也是全球自動駕駛領域目前所達到的最高等級。以下大致回顧和展望汽車產業從ADAS到全自動駕駛的發展歷程。



*圖1 自動駕駛不同等級可以實現的功能及時間預測。(資料來源：Arm)*

國際汽車工程師學會(SAE International)定義了Level 0~5六個自動駕駛等級。其中Level 0完全沒有駕駛輔助控制功能，本文從Level 1開始到Level 5大致介紹這五個等級，從先進駕駛輔助系統和完全自動駕駛的區別。

·Level 1和Level 2以人自主駕駛為主，ADAS為輔。大約從2000年開始，Level 1等級的駕駛協助工具開始出現，包括自我調整巡航控制(ACC)、車道保持、自動緊急煞車系統(AEB)和平行停車(parallel parking problem)協助等。2013年開始出現Level 2等級的部分自動功能，包括方向盤自動控制、換道、交通堵塞協助等，特斯拉AutoPilot系統就屬於Level 2等級。

·2018年出現的Level 3等級實現了有條件的自動駕駛，即需要人和車同時參與。但這在人類行為習慣和法律裁定方面都難以協調，因為一旦不需要全神貫注地開車，人們就會分神，在出現緊急情況車輛需要人工參與時很難及時做出反應，甚至有可能因為駕駛不知道自己是否應該介入而導致事故。很多OEM和技術公司都聲稱越過Level 3，直接進入Level 4，因為無論從法規還是技術角度Level 3都比較有挑戰；但是，從研究和學習的角度還是有其價值。

·Level 4和Level 5以車為主，人基本或完全不參與。Level 4等級即可實現高度自動化，解放出人的眼、手和腳，車輛可以在高速上自動行駛達到100英哩/小時，實現自動換道和自由行駛，預計2024年進入商用部署階段。Level 5是真正的全自動駕駛，預計2027年自動駕駛計程車(Robo-Taxi)和無人駕駛穿梭巴士開始提供交通運輸服務，人們可以在任何環境條件下自由乘坐，但目前還沒有廠家達到Level 5等級。

從原型測試到量產和商用部署面臨的挑戰

無論網際網路巨頭、汽車OEM，還是自動駕駛技術公司，目前都在原型測試和驗證階段，自動駕駛離批量生產和大規模商用部署還有很長的路要走。從非技術層面來說，所面臨的挑戰在於高昂的成本和消費者心理接受程度；從技術角度來看，面臨的難題包括多感測器融合所需要的高性能處理運算能力、複雜的軟體和演算法，以及自動駕駛所要達到的功能性安全(Functional Safety)及資訊安全(Information Security)。

·自動駕駛車輛成本居高不下。實現Level 4和Level 5等級自動駕駛的車輛要比普通車輛額外花費7.5~10萬美元，只有交通行動服務(Mobility-as-a-Service；MaaS)營運商才能支付得起，還遠遠高於普通消費者的支付水準，而各種類型的感測器是導致高昂成本的主要因素。

·消費者心理接受程度：對自動駕駛車輛安全的擔心是消費者不願接受自動駕駛的主要原因。調查統計顯示，超過60%的受訪者不但不願意乘坐自動駕駛車輛，也不願意在路上跟自動駕駛車輛共用道路。要建立對車輛功能安全性的信任還需要時間，另外消費者也擔心連網的車輛會遭受駭客攻擊和破壞。

·複雜繁多的感測器和資訊輸入源：光達(LiDAR)、車載雷達、攝影機、影像處理、電腦視覺等大量資料的輸入和融合需要分類處理、做出即時決策和採用相應行動。

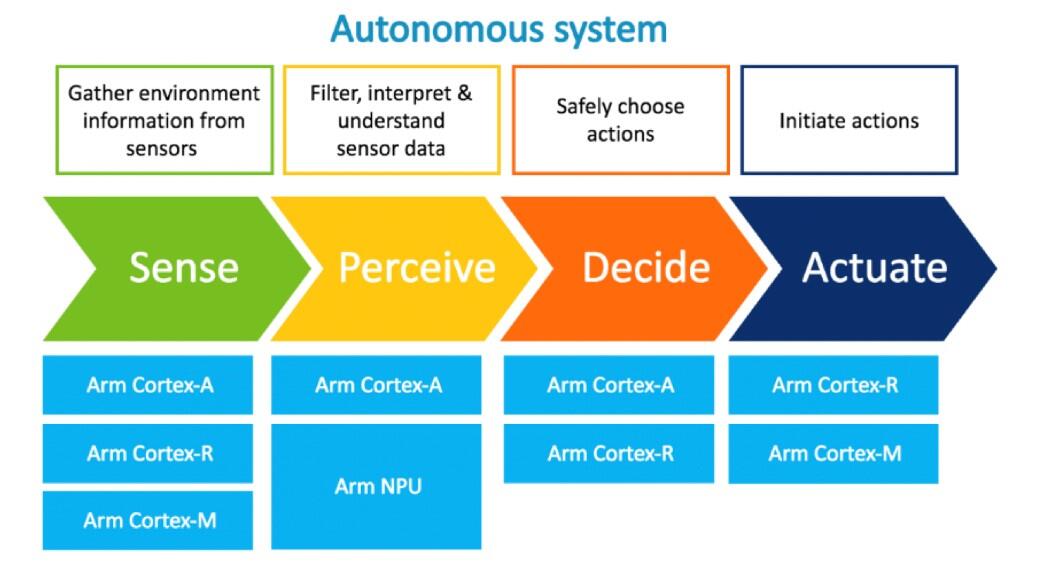
·軟體和演算法的複雜性：一個能夠實現完全自動駕駛的車輛大約需要10億行程式碼的軟體，這是任何一家公司都無法獨自完成。和飛機做個對比，波音787 Dreamliner的軟體才包含1,400萬行程式碼，因為飛機的飛行環境和路徑相對簡單，而且飛行員都是經過專業訓練的駕駛。而自動駕駛車輛的運行環境要複雜得多，不但要在擁擠的道路上與其他車輛互動，而且要隨時注意行人，還要應對各種各樣的天氣和路況。

·異質整合的高性能處理器支援：感測器融合(Sensor Fusion)和影像處理對CPU、GPU和專用AI加速器提出了極高的要求。此外，處理器和整個系統的功耗和尺寸也要大幅度減少。

·功能性安全：目前業界還沒有統一的功能性安全標準，各種安全性技術雖然已經經過驗證，但仍無法滿足自動駕駛對功能性安全的要求。

運算性能要提升10~100倍

對多輸入來源的感測器資料進行即時處理是自動駕駛系統對處理器硬體和軟體提出的高要求。資料處理分為四步：感測(Sense)、察覺(Perceive)、決策(Decide)和致動(Actuate)。

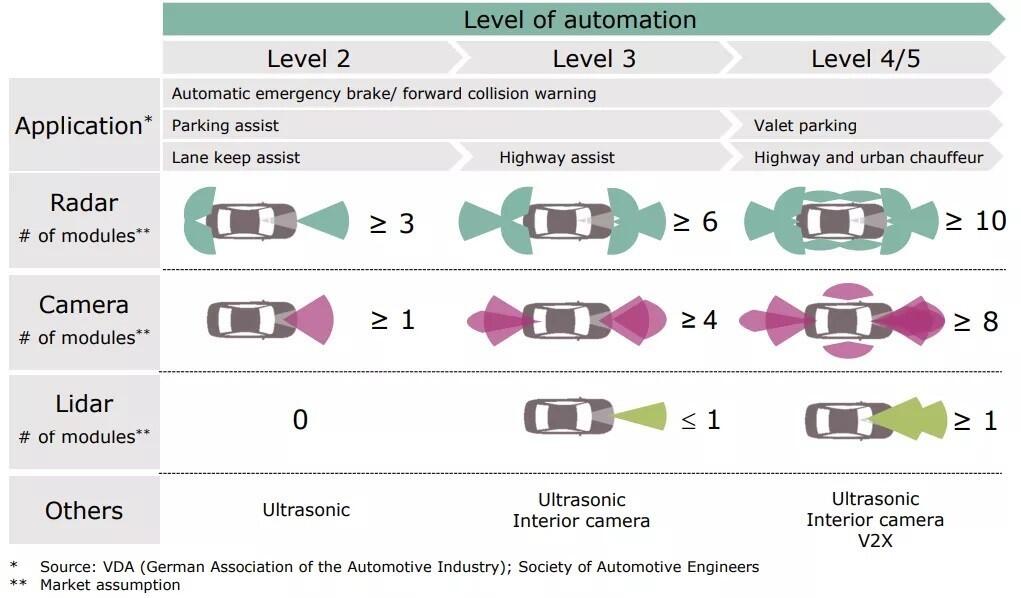
*圖2 自動駕駛系統處理資料的步驟。(資料來源：Arm)*

鑒於自動駕駛對資料處理性能的要求和軟體及演算法的複雜性，Arm汽車解決方案和平台總監Robert Day認為，若採用統一的自動駕駛運算平台，業界就可以更好地協作開發硬體和軟體系統，確保安全一致性，而且可以降低整體成本，加速自動駕駛從原型測試到批量生產、規模化部署和商業化營運的發展步伐。Arm最近聯合Nvidia、NXP、GM、豐田和博世(Bosch)等業界廠商聯合成立自動駕駛運算聯盟(AVCC)就是基於這一理念。

據Day介紹，Arm CPU、GPU、ISP和NPU等系列IP使得基於Arm的晶片解決方案可以在整個車輛中使用，而Arm的半導體合作夥伴提供了廣泛的汽車級SoC。Arm完整的處理器系列包括應用處理器(Cortex-A)、即時處理器(Cortex-R)和小型低功耗微處理器(Cortex-M)，以適應自動駕駛系統的所有階段。隨著Arm的半導體合作夥伴將更多運算元素加入異質SoC平台，將有助於滿足自動駕駛的運算處理要求，同時有助於降低功耗、價格、尺寸和散熱。

這些離散的感測器包括：光探測和測距(光達)，用脈衝雷射測量到目標的距離；無線電探測和測距(雷達)，使用無線電波代替雷射；紅外線(IR)攝影系統，使用熱成像技術在黑暗中進行感測，以及普遍採用的攝影機系統等。

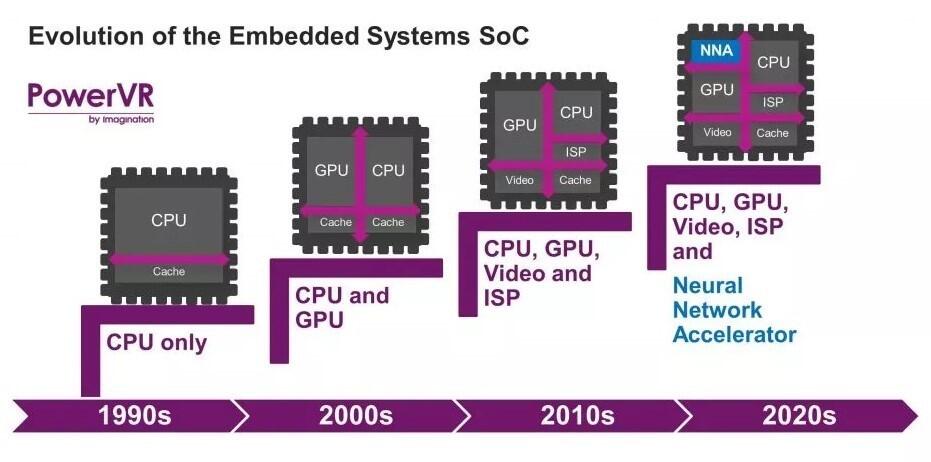
某些資料可以在感測器本地處理，但大部分數據都要透過感測器融合來彙聚、過濾和分類。感測器融合要處理TB量級的資料，這是通用型CPU無法滿足的，但GPU可以提供10倍於CPU的性能， 非常適合自動駕駛和ADAS技術對處理能力的要求，尤其是在影像分析和平行訊號處理方面，自動駕駛系統可以利用GPU的圖形運算能力去即時處理和分析感測器資料。



*圖3 自動駕駛的不同等級所需要處理的感測器類型和數量。(資料來源：Imagination)*

在上世紀90年代，CPU增加了浮點運算單元和快取記憶體以提高性能，此後GPU也被整合至CPU中。到2010年代，影像訊號處理器(ISP)和對視訊轉碼器的硬體支援也加入進來。現在則輪到神經網路加速器整合進晶片，實現晶片自身的最佳化，並成為網路邊緣運算設備的標準組成部分。

隨著AI、神經網路和深度學習的興起，針對特定領域的專用加速器NPU則可以將運算性能提高200倍。所有這些使得ADAS/自動駕駛系統能夠更好地解析環境，並且可提升系統輔助駕駛和維護自動駕駛車安全性的能力。隨著自動駕駛從Level 2級提升至Level 4和Level 5，越來越需要車內系統能夠對車輛所行駛的環境有更詳細、更廣泛的瞭解。

*圖4 嵌入式系統SoC的演化。(資料來源：Imagination)*

據Imagination公司汽車業務總監Bryce Johnstone介紹，PowerVR GPU和神經網路加速器可以解決自動駕駛平台開發人員面臨的資料處理和可信架構挑戰。此外，PowerVR GPU支援完全的硬體虛擬化，將共用GPU的虛擬實例進行徹底的隔離。從而可以有效地驅動ADAS/自動駕駛平台架構的發展，同時提供實現安全、可靠的自動駕駛處理所需的強大性能。

功能安全要達到ASIL D等級

根據ISO 26262規範的定義，功能安全性是指即便電氣和電子系統因為故障導致損壞，但也不會給車輛帶來無法預測的安全風險。ISO 26262對車輛安全完整性等級(ASIL)從低到高劃分為四個等級，即ASIL A、B、C、D，這些安全等級跟特定系統監測出的故障次數有直接關係。

據統計，超過90%的車輛事故都是人為失誤造成的，如果自動駕駛車能夠達到所期望的安全等級，嚴重交通事故將有望大幅度減少。然而，自動駕駛系統需要極高的運算性能和最高等級的安全性以確保車輛高速行駛的安全，在功能安全性方面有哪些技術可供選擇呢？

鎖步和拆分-鎖定

從晶片和硬體的角度，實現功能性安全所涉及的技術包括內建自檢、同位、鎖步(Lock-step)、錯誤監測/糾正，以及看門狗等。其中鎖步和拆分-鎖定(Split-lock)是兩個可以同時滿足自動駕駛性能和安全性要求的安全技術。

在「鎖步」中配置兩個CPU核心是實現高水準診斷的傳統方法，即能夠檢測到錯誤情況的發生。其原理非常直截了當，每個核心饋入比較器邏輯塊，並且每個核心執行完全相同的程式碼，比較器邏輯逐個週期比較輸出，只要結果相等，一切就OK。如果結果之間存在差異，則表示有安全隱患，應該進一步監測或採取措施解決故障狀況。這種「鎖步」機制是透過設計固定在晶片裡的，因此靈活性不夠。因為運作應用程式要使用兩個核心，只能獲得單核心的性能，這種方法已被「證明」可行有效，並已在微控制器和不太複雜的確定性微處理器上使用多年。

據Day稱，Arm在車用級微處理器核心Cortex-A76AE和Cortex-A65AE中導入了「拆分-鎖定」安全機制。拆分-鎖定允許在啟動時將系統組態為「分離模式」(兩個獨立的CPU，可用於處理不同的任務和應用)，或「鎖定模式」(針對高安全完整性應用，CPU處於鎖步模式)。這種「拆分-鎖定」功能對於自動駕駛系統至關重要，可以實現出色的運算性能和高度的安全完整性支持。

**本文為EE Times China原創文章**