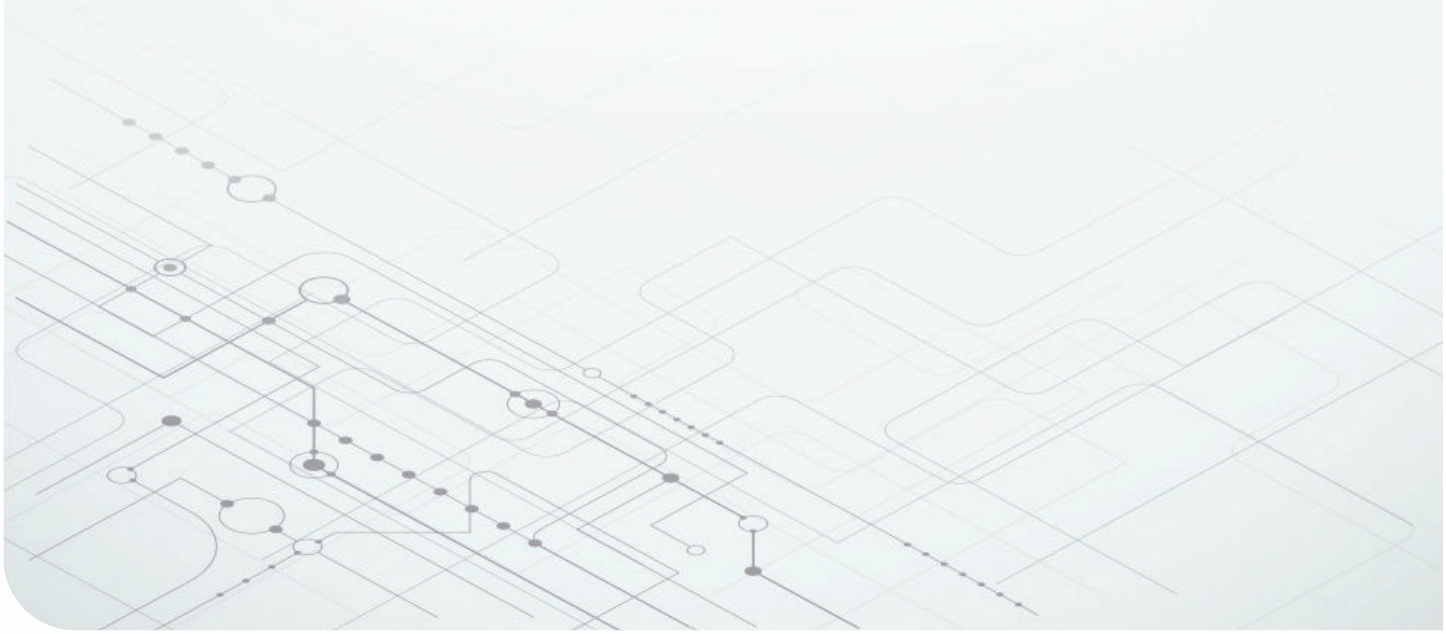
參考

確保 Arm 式應用處理器的安全

Texas Instruments

Amrit Mundra
Security Architect and Systems Engineer



簡介

電腦安全性過去意指 PC 上的惱人病毒。隨後風險提升。駭客入侵商業和政府系統，代表個人和金融資訊都會暴露在詐欺、盜竊和貪汙風險下。不過，現在嵌入式系統的安全性 (或者更準確來說，是嵌入式系統的不安全性)，會對極度重要的數據造成威脅。

現今的世界需仰賴數據運作，每個位元或位元組都應視為潛在的攻擊目標。同時，軟體和硬體系統也變得更加複雜、緊密連結且相依。而弱點也伴隨著複雜性而來。數十億或數兆行的程式碼，以及相互關聯的硬體模組、子系統和分割區，全都擠在微小的矽片上，讓駭客開心不已。

當然，駭客不會靜止不動。關於嵌入式系統弱點的報告源源不絕：衛星通訊系統、無線基地台、住宅和公司中的雷射印表機、智慧電網、除顫器等醫療裝置，以及許多其它系統，全都面臨風險。多年經過，對多核心嵌入式晶片系統 (SoC) 的安全性需求只增不減。心臟用設備、智慧型手機和汽車控制單元等嵌入式裝置，皆需仰賴包含嵌入式 SoC 在內的多種元件，以保護控制中心。

首先，我們會介紹為了協助保護嵌入式系統中具有多個核心 Arm® 式應用處理器，所需採用的這類要件。接著，我們會對這類處理器的基礎安全層，也就是安全啟動，進行更詳細的探討，因為有了安全啟動，才可從「開機」起即保護系統。如果沒有採用安全啟動，那麼系統在從「開機」到使用之間，將會出現間隙。由於威脅的本質瞬息萬變，因此安全性一直都是不斷變化的目標。

就系統的安全性層面而言，其目標在於保護系統免受駭客攻擊，因為駭客會想要竊取數據或接掌系統，以透過不同於預期的方式來使用系統。這與功能安全的相關概念不同。安全較著重於確定系統能以有組織的方式回應各種情況，並且可在需要時平穩地當機。結合這些概念，代表在這個會發生損壞且存在不法分子的現實世界中，系統仍能以符合預期的方式運作。

風險管理

安全性威脅一直存在，且隨着物聯網 (IoT) 快速普及，這類威脅可能來自任何位置，甚至是不顯眼且低成本的終端節點裝置。基本的安全性問題並非系統是否會受到攻擊，而是系統何時會受到攻擊。對此得到的結論是就安全性而言，風險管理與保護一樣重要。

由於系統可能受到攻擊，系統設計人員該如何將安全漏洞的風險降至絕對最低的程度？

該保護什麼？

任何寶貴之物都可能受到攻擊。當然，根據駭客的觀點和企圖而定，幾乎所有一切都可視為寶貴之物。就最原始的層級而言，對大部分駭客社群來說，侵入系統所獲得的純粹快感就十分寶貴。大多數駭客都不是想尋求刺激的無害人士。許多駭客會毫不猶豫地將手探入電子錢包，或是竊取如信用卡和銀行帳號等金融資訊，以用於詐騙。IP 可能遭竊取以供出售或獲取競爭優勢，而政府機密則可能遭濫用並用於中斷、破壞或摧毀運輸系統、供水系統、能源分配網路、核電廠，以及國家公共基礎設施的其它層面等。

當然，所有這些寶貴之物都必須受到保護，但在可加以保護之前，安全性系統本身必須安全無虞。就嵌入式系統而言，必須為系統內的安全性元件及系統保護的項目提供防護。以最基本的層級來說，這代表需保護用於驗證軟體、使用者和連線連結的密碼編譯金鑰和身分。這也代表需確保在網路中每個系統或節點上執行之軟體的完整性。而這需要能掌握並控制開機與執行階段軟體，即使是在網路或網際網路中最不起眼的節點上，也不例外。

安全性的成本多高？

就像其他一切一樣，安全性會帶來成本。系統開發人員的安全性成本，包括設計安全性措施並將其整合至系統的成本，以及這些安全措施會對系統性能加諸的影響。由於安全性威脅的本質瞬息萬變，且嵌入式系統也透過物聯網等措施持續普及，因此新系統的設計作業應包括開發一套指標，以根據其優勢來衡量安全性成本。嵌入式裝置可能遭到接掌並做為起點，以攻擊可能安置了更多寶貴資源的其它系統。例如，駭入印表機 / 影印機可能不會為駭客帶來極高價值，但如果印表機列印或複製的每份文件都遭到擷取並傳送給駭客，就可能造成龐大損害。

就安全性成本而言，嵌入式系統具有優勢，因為許多以嵌入式系統為基礎的產品都是大量生產的產品。因此，針對這類產品所開發的安全性子系統成本，即可攤銷至大量的生產作業中，進而降低每單位安全性成本。此外，針對新設計所開發的多功能、可擴展和可攜式安全性架構，通常

可以移轉至密切相關的系統，或是可稍加修改該架構，以滿足其它產品的需求。

架構考量

許多安全性子系統都採用分層架構，並且會善用劃分功能。在各層部署安全性措施，可對系統的安全性帶來累積性影響，因為在採取行動之前，每一層都可先確認其下層或上層的安全性。為了確保在系統上執行之軟體的執行階段安全性，劃分至關重要，且劃分也讓設計人員能根據受保護之資源或程序的相對價值，量身打造安全性措施。

嵌入式安全性始於硬體。 相較於任一解決方案單獨運作的情況，若能結合軟體和硬體安全性功能，即可實現更加安全的保護層。此外，廠商提供的工具可簡化安全性子系統的開發作業，並確保所造就的架構符合開發人員的要求。例如，硬體式安全加速器可降低安全性子系統的性能成本。

當然，安全性架構的優勢取決於其建置基礎。基礎層有三項不可或缺的層面：安全開機程序、硬體式裝置 ID / 金鑰，以及密碼編譯加速。

安全性金字塔

安全性金字塔 (請參見圖 1) 說明了在多核心 SoC 嵌入式處理器的全方位安全性子系統中，各個不同層面與構成要件。

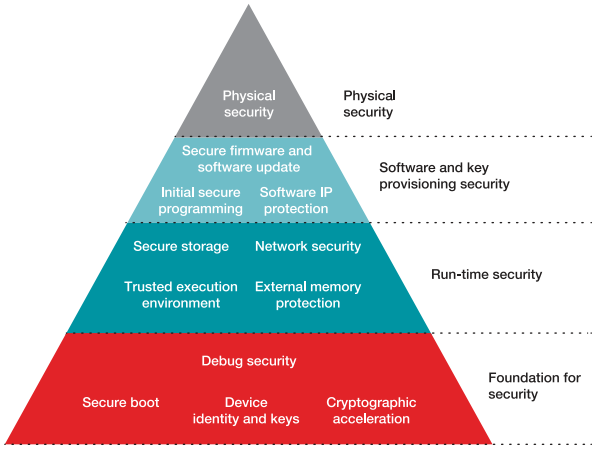


***圖 1.** 安全性金字塔。*

安全啟動

安全啟動程序可為嵌入式系統建立信任根。即使是從外部快閃記憶體啟動，安全啟動程序也可透過任意數量的機制 (如嵌入式密碼編譯金鑰與其它方式) 來驗證啟動韌體的完整性。安全啟動層可防止惡意軟體接掌系統、任何可能複製系統內 IP 的行為、非故意地執行不需要的應用，以及其它安全性風險。

安全啟動也可透過加密 IP 與安全複製 IP，協助提供額外的保護層，進而保護內部記憶體。擁有加密能力，也可為程式碼庫提供更多安全性，因為如此可禁止進行定向探索攻擊。

最重要的是，安全啟動可協助奠定嵌入式系統安全性的基礎。

加密加速

密碼編譯處理包含各種公開金鑰和私密金鑰的產生、驗證和認證，而密碼編譯處理可能會對嵌入式系統的性能和處理能力造成負面影響。部分多核心應用處理器配備硬體式加速器或協同處理器，可大幅加快編碼 / 解碼程序。雖然也可使用軟體式加速，但軟體本身的固有安全性無法媲美硬體式密碼編譯加速。

常見的密碼編譯要素	
隨機數字產生器 (RNG)	密碼編譯演算法及雜湊函數會使用。硬體產生的隨機數字比軟體產生的 RNG 安全。
密碼編譯演算法	
三重數據加密標準 (3DES)	3DES 會執行 DES 加密三次，以強化對加密數據的保護，並解決 DES 演算法的部分弱點。
公開金鑰演算法 (PKA)	速度加快的 PKA，使用採用公開 / 私密金鑰的 RSA 或 ECC 非對稱加密。可協助進行安全啟動所使用的驗證作業。
先進加密標準 (AES)	AES 是現今廣泛使用的最先進密碼編譯演算法之一。
雜湊函數 (適用於簽名、驗證等)	
訊息摘要演算法 (MD5)	雖然此雜湊函數已受到廣泛部署，但其在部分應用中具有特定弱點。
安全雜湊演算法 2 (SHA2)	可處理大型雜湊，因此比 SHA1 安全。

***表 1.** 常見的密碼編譯函數範例。*

裝置 ID 和金鑰

為了信任透過區域網路 (LAN)、廣域網路 (WAN) 或網際網路進行的通訊，裝置必須具有可分享的唯一身分。隨後通訊裝置即可判斷參與對話的其它裝置真實性或可信度。

應用處理器通常隨附某種類型的唯一識別 (ID) 代碼。此外，或是除了 ID 代碼之外，裝置可能會透過簽名或憑證金鑰以識別自己的身分，且前述簽名或憑證金鑰會具有可透過雲端服務等方式存取的對應公開金鑰。

圖 2. *裝置 ID 有助於防止遭竊。*

偵錯安全性

在系統開發期間，設計人員需要可存取嵌入式多核心應用處理器，以對韌體和軟體進行偵錯，以及對可能的硬體問題進行疑難排解。在大多數情況下，可提供前述存取功能的連接埠是 JTAG 埠。在操作環境中，偵錯埠必須透過某種保險絲密封，或是只能透過經認證的密碼編譯金鑰進行存取。否則偵錯埠可能會為駭客提供易於進入系統的方法 (請參見**圖 3**)。

圖 3. *MSP430™ MCU 偵錯埠。*

可信執行環境

執行階段安全性層由數種不同的功能組成，而在啟動程序之後以及系統的作業系統 (OS) 執行期間，前述功能均可協助保護系統。執行階段安全性的重點之一在於監控系統的所有層面，以判斷發生入侵或嘗試進行入侵的時間。

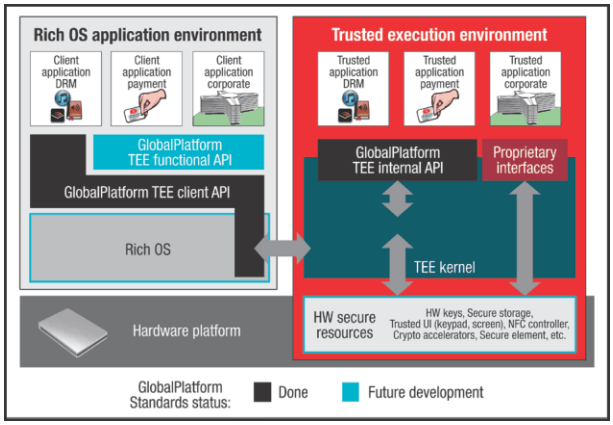


圖 4. *可信執行環境 (TEE)。*

可信執行環境安全性讓系統能同時代管安全和非安全應用，並透過系統維護分割區，進而避免洩漏數據。重點在於執行敏感應用時，應透過沙箱方式完全將應用與相關程式碼 / 數據庫隔離。

可信任執行環境基本上可在多核心系統內提供受到安全保護的分割區，且其中只可執行經認證的安全韌體、軟體和應用，並且可儲存經認證的數據。

將可信執行環境與多核心 / 多處理系統的其它部分隔離，可防止可能侵入系統的可疑程式碼、應用和數據汙染關鍵任務軟體、數據和其他 IP。

外部記憶體保護

當設計人員必須對系統新增其他應用或子系統時，通常必須新增位於主處理器外且透過記憶體匯流排連接至主處理器的記憶體。設計人員必須保護儲存在外部記憶體中的數據，使其免於遭到竄改或更換，以確定只有受到信任的數據或應用程式碼會儲存至外部記憶體中。我們可採用多種方法來保護外部記憶體的內容，例如從外部記憶體進行安全的晶片內執行作業，不將數據載入處理器的整合式記憶體中；進行即時解密，以在讓應用程式於主處理器上執行的同時，亦能維持機密性，以及其它方法等。

圖 5. 安全的記憶體。

網路安全性

駭客非常擅長攔截無線或有線網路通訊。事實上，部分通訊協定具有已遭到利用的已知安全性弱點。僅部署高度安全的通訊協定通常需要大量的處理週期，以加密和解密通訊流，以及驗證傳送者或接收者的真實性。設計人員有時需在通訊輸送量與安全性之間取得平衡，不過部分嵌入式處理器整合了可提供密碼編譯演算法的硬體式加速器，可搭配標準通訊協定使用，進而避免陷入這種兩難情況。

圖 6. 安全儲存。

安全儲存

密碼編譯金鑰和安全性數據，均必須儲存在系統記憶體中不會受到不必要存取的位置。我們可使用多種功能以提供安全的儲存方式，包括加密金鑰 blob、只能透過主要金鑰解鎖的防篡改防護功能、在非揮發性記憶體和加密引擎間的私密金鑰匯流排等。

初始安全編程

在現今的全球化時代，設計、金鑰佈建和製造均無相連，有時甚至距離跨海之遙，這也為確保金鑰等安全性資產的安全無虞，帶來挑戰。而讓情況更加複雜的是，商業模式可能包含採用完全不受信任之製造設定的 ODM。

如初始安全編程等安全性功能提供了可讓客戶評估與選擇使用的方法，以針對在不受信任設施或第一次啟動應用期間所編程的初始韌體或金鑰，強化其機密性、完整性及真實性。

安全的韌體和軟體更新

在安全性架構中，更新系統的能力是重要環節，其可為客戶提供遠端修補或更新軟體的機會，以對應系統中已識別的弱點，然而在更新期間，最大的挑戰在於需阻止間諜、假冒和重放。

安全性架構提供可加以部署的額外金鑰和機制，例如驗證、加密和完整性檢查等，以確保更新的真實性。

軟體智慧財產 (IP) 保護

客戶挹注了大量投資以創造智慧財產 (IP)，而智慧財產可能代表了對市場終端使用者的關鍵價值主張，因此，安全性架構必須提供如加密啟動、可執行隔離式處理的能力以及防火牆等機制，讓客戶能保護其 IP。

實體安全

眾所周知，老練和沒那麼老練的駭客組織會從系統中移除晶片，或是從晶片封裝中移除矽晶粒，以存取嵌入式資產。

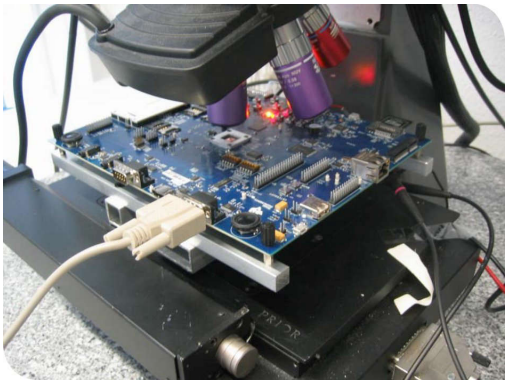


圖 7. 受到實體攻擊的系統。

移除裝置或晶粒後，駭客即可對其大肆攻擊，包括使用雷射、對其供電至超出規定的功率限制，或使用其它手段等。其目的在於觀察裝置對刺激的反應，因為這類回應可能會洩露弱點，駭客隨後即可利用這些弱點來存取裝置。

部分應用處理器已整合硬體和軟體功能，以阻擋這類針對 SoC 數位和類比區段的實體入侵。整合至多核心應用處理器中的篡改防護模組可能包含電源和溫度監視器、重設功能、頻率監控器和可編程篡改防護功能。

機殼保護

機殼保護功能是可針對包覆系統的機殼提供防護的實體措施。從鎖定機制，到電子開關、可斷線路跳脫機制等等，都屬於這類功能 (請參見**圖 8**)。

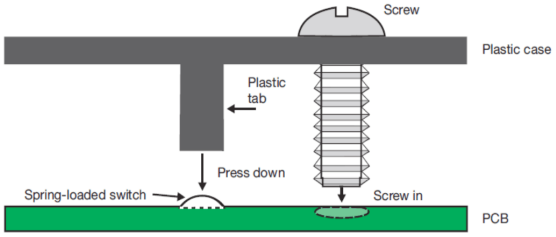


***圖 8.** 機殼保護。*

嵌入式安全性應從何處著手？

嵌入式多核心應用處理器的安全性基礎始於硬體。如果硬體不安全，那麼無論安全性軟體數量多寡都無濟於事。假設安全性功能已內建至硬體，那麼著手建置安全性子系統時，首先應著眼之處就是在開機後執行的第一個軟體，也就是啟動程式碼。如果無法驗證啟動程序，也就無法驗證在系統上執行的任何其它軟體。因此，保護啟動程序安全無虞，是系統中所有安全性所仰賴的支柱。

安全啟動程序可建立信任根，而這是每個安全性子系統的目標。透過安全啟動程序建立信任根，有助於確保系統的完整性，並防止駭客接掌系統的任何部分。這也有助於保護系統中的客戶軟體，並且可做為反複製屏障，讓系統或其任何部分均不會遭到複製。

安全啟動程序通常包含將公開密碼編譯金鑰編程至位於系統某處的非揮發性、一次性可編程記憶體中。隨後，此公開金鑰必須與啟動程式碼相關的私密 / 公開金鑰匹配，才能在開始執行前，驗證加密啟動程式碼的有效性。啟動韌體可載入至嵌入式處理器的 RAM，或是若要提高安全性，則可從位於嵌入式處理器之外的記憶體加以保護並於晶片內執行。部分韌體映像是由多種元件或模組組成。要求在解密和執行每個模組之前進行驗證，即可強化啟動安全性。

TI 應用處理器的安全性功能

我們的 Arm 式應用處理器提供一套全方位的安全性功能，可協助開發人員實作其安全性措施，以保護資產 (數據、程式碼、身分和金鑰)。

安全性功能	AM335x	AM437x	AM438x	AM570x/AM574x	AM64x/AM65x	AM62x	AM68x/AM69x	DRA821/ DRA829/ TDA4VM
加密加速	✓	✓	✓	✓	✓	✓	✓	✓
裝置身分/金鑰	✓	✓	✓	✓	✓	✓	✓	✓
安全啟動	✓	✓	✓	✓	✓	✓	✓	✓
偵錯安全性	✓	✓	✓	✓	✓	✓	✓	✓
外部記憶體保護			✓		✓	✓	✓	✓
可信執行環境 (TEE)		✓	✓	✓	✓	✓	✓	✓
網路安全性					✓	✓	✓	✓
安全儲存		✓	✓	✓	✓	✓	✓	✓
軟體 IP 保護	✓	✓	✓	✓	✓	✓	✓	✓
初始安全編程	✓	✓	✓	✓	✓	✓	✓	✓
安全的韌體更新	✓	✓	✓	✓	✓	✓	✓	✓
實體安全			✓					
申請	聯絡 TI 代表	更多資訊	更多資訊	更多資訊	更多資訊	更多資訊	更多資訊	更多資訊

***表 2.** TI 應用處理器的安全性功能。*

結論

嵌入式處理器安全性是多面向的複雜主題。隨著物聯網興起和嵌入式系統普及，相較於過去，現在駭客擁有了大量主要目標。

當然，硬體中必須具備基礎安全性功能，但若要為嵌入式多核心 SoC 建置安全性子系統，應從安全啟動的基礎層著手。如果沒有安全啟動程序的信任根，任何其他安全性措施都於事無補。建立此信任根後，系統安全性的其他面向，例如偵錯安全性、執行階段安全性和網路安全性，即可獲得穩固的基礎。否則，所有安全措施都只能建立在搖搖欲墜的基礎上。

參考

1. 德州儀器：***電子書：建置應用時應考慮安全性***
2. 德州儀器：***透過硬體加速密碼編譯實現安全性並提升晶片性能***
3. 德州儀器：***嵌入式 Sitara™ 處理器的安全啟動***
4. 德州儀器：***Sitara AM438x 處理器：篡改防護***

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265