白皮书

面向工业和物联网应用的高性能、高度安全的网络

摘要

网络、工业控制、机器对机器(M2M)和新兴物联网(IoT)市场都共同存在着一项类似的基本要求：能够安全且可靠地连接丰富多样的端点，并且支持网络范围的集中式控制功能。在企业网络中所用的互联网协议(IP)标准如今也广泛应用于工业自动化、M2M和物联网(IoT)市场，这允许这些行业能在新兴应用领域中充分发挥的通用网络构建模块的优势。本白皮书将会探讨旨在确保工业、M2M和物联网(IoT)网络组合支持的一些附加要求，从而实现信任度、安全性、高可靠性和高效性能的目标。

目录

freescale™ 飞思卡尔

前言

网络、工业控制、机器对机器(M2M)和新兴物联网(IoT)市场都共同存在着一项类似的基本要求：能够安全且可靠地连接丰富多样的端点，并且支持网络范围的集中式控制功能。广泛应用的互联网协议(IP)标准可以支持工业自动化、M2M和物联网(IoT)市场，从而充分发挥通用网络构建模块的优势。

制造商在寻求更高的数据可见性，希望提高生产能力并且远程管理他们的工业操作，以太网应用可以支持工厂车间机器之间的连接性，这一需求一直在稳步增长。增强工厂联网设备的可见性和管理能力，有助于精简各种相关的功能，这取决于能够确保工厂网络范围所载数据的安全性。

作为二十多年一直服务于控制层和数据层应用的网络处理器顶级供应商之一，飞思卡尔继续在引领这一行业趋势的发展。无论设计涉及网络基础架构、工业控制网络（网关或PLC）或工厂车间设备，必须满足一些基本要求：交付出色的可靠性、数据安全性、高效数据包处理和性能增强的连接支持能力。

飞思卡尔凭借其基于Power Architecture®技术的通信处理器支持上述需求，首先确立了自身作为网络解决方案领先者的地位。秉承过去二十年获得的专业技术和创新记录，飞思卡尔推出了第一款基于ARM® ISA的QorIQ网络处理器系列产品。创新的QorIQ LS1021A处理器配置了两个高效ARM Cortex®-A7内核，带有ECC保护的L1和L2高速缓存，确保达到最大化可靠性，并支持高达1 GHz的运行速度。这款ARM双核提供了在功耗3W以下的微处理器前所未有的集成水平。高性能网络接口包括千兆以太网、PCI Express® 2.0、SATA 3.0和USB 3.0。LS1021A处理器还可以支持旧有串行接口，其中包括TDM、HDLC、UART、I2C、SPI、CAN和PWM/Quadric解码。除了丰富多样的通信接口之外，该处理器还可以支持SDHC、I2S和集成LCD控制器。

通信加速器

在过程自动化和制造业控制应用中，网络必须永远可用、高度可靠且具有安全性。与此同时，网络处理器需要提供智能功能，让众多公司充分利用如现今网络提供的信息流优势。

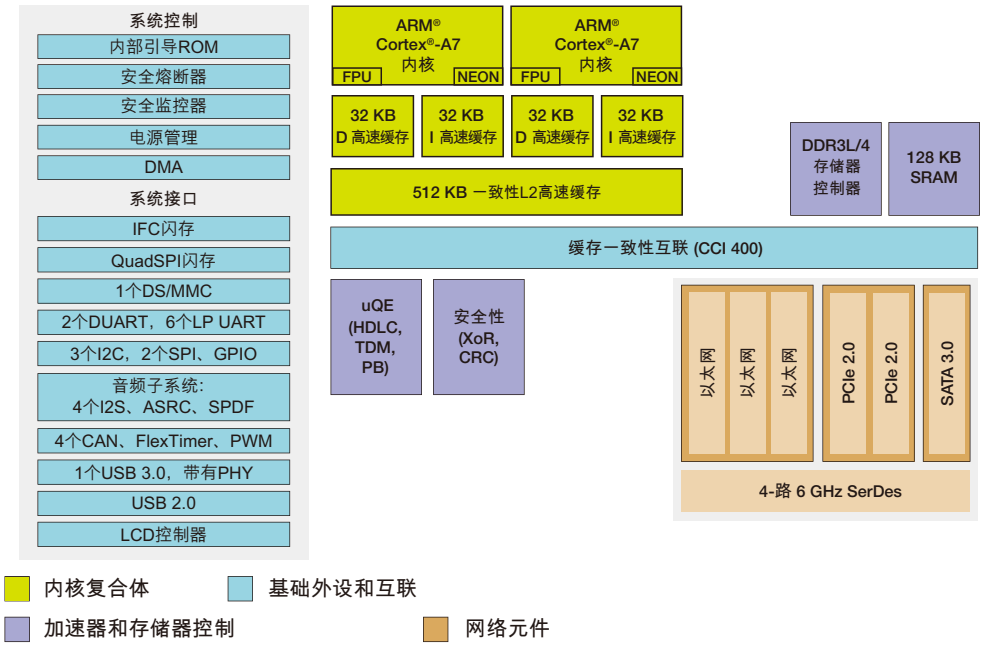
为了交付最大可靠性和强大的安全性，飞思卡尔网络处理器集成了业界领先的网络加速和保护技术。这些技术便是可编程的微型QUICC引擎，可以支持Field Bus和RS485协议，例如PROFIBUS（包括主机和从机），以及旧有HDLC和TDM通信协议。

支持以太网连接性，每一个虚拟化、增强三倍速度的以太网控制器(VeTSEC)可以支持进出口的IEEE® 1588时间戳，结合硬件内部的计时器和脉冲实施。硬件还支持软件受管队列，

与ISO第4层的入口解析和硬件出口优先次序相结合，可以实施简单有效的排队任务。

这些公认的以太网控制器都通用于工业应用的其它飞思卡尔处理器中，拥有丰富多样的成熟软件驱动程序支持，其中包括面向工业以太网(EtherCAT® Master)、PROFINET® (RT)、EtherNet/IP™和PRP的软件栈。

QorIQ LS1021A 处理器结构图



以太网族系功能

QorIQ LS1021A处理器的设计旨在彻底满足苛刻和恶劣条件下网络应用的需求。这个目标可以通过向所有存储器融合错误检测和纠错(ECC)技术而实现，其中包括第1层和第2层高速缓存以及SRAM、外部DDR存储器和看门狗定时器，从而获得最大可靠性。通过ECC保护的存储器可以完善可靠性，高性能安全引擎支持全系列的数据保护机制，包括安全启动、可靠架构、ARM TrustZone®和生产保护，结合起来可以提供最大化的可靠节点能力。

这些功能都是物联网(IoT)应用的必要条件，在其中许多边缘网络设备和传感器将会捕捉和传输各个节点之间的特定用户数据。因为这种数据可以直接关联或链接到单独的用户，数据必须经过加密处理。这日益受到法规的监管与监控，扩展到所用加密标准和协议的技术规范。不可避免的是，这会要求M2M或物联网(IoT)应用中所使用的通信处理器必须具备执行加密操作的功能，例如哈希算法、签名和加密数据，以及旨在满足法规要求的安全密钥存储单元。

工业通信线路也必须具备安全性，不仅是为了防止数据探测，而且也在于防止非授权控制，导致发生代价高昂的事件，例如生产线停产等。

然而，即使网络通信线路之间传输的数据经过加密处理，物理设备仍然无法抵御程序软件非授权修改的攻击。因此，设备不仅必须提供安全的通信，而且还要能够作为可靠节点运行。可靠节点就是用户可以完全依赖的设备，它不仅可以保护数据，而且确保只能执行用户创建的真正软件。

在真实世界中，信任通常都是商议达成的，这个观念可以类似的方式扩展至数字领域。如果您通过可靠来源获得信息（数据或命令），您可以认定它是可靠、有效的信息。启动可靠设备需要一个“可信根”(“root of trust”)，它可以是外部（通常成本高昂）设备，例如FPGA或ASIC；或者它可以集成到SoC（片上系统），比如它便安装在QorIQ LS1系列产品之内。在LS1021A处理器中，验证是在预引导加载器中执行的，它完全包含在内部ROM之中。这种实施方案可以提供一次性用户可编程验证密钥，结合预引导加载器使用，创建所需的可信证明，以防止非授权代码/用户控制系统。可信节点功能可以通过编写验证密钥和启用位实现，这是一次性用户可编程保险。一旦可信模式启用，外部引导代码映像（例如引导加载器、OS内核或裸机代码）将会只能在预引导加载器密钥解密和验证之后执行。然后这一代码会成为下一个可信源。包括解密/验证代码在内，可以成为类似数据的密钥，应用在可信通信线路。支持主签名代码映像和备用（附属）签名代码映像，以便提供附加的可靠性。

外部代码映像加密采用与用户开发团队相同的密钥，都是使用编程设备提供的工具链编程QorIQ LS1021A处理器上密钥区域的集成密钥。因此，当代码离开开发小组时，已知代码映像具有安全性。

一旦代码映像通过设备的验证，设备便会在“安全”状态下运行。为了维护安全的运行状态，处理器需要提供附加的安全功能，以便检测和防止非授权篡改或外部存储器控制代码/数据。

安全调试控制器通过JTAG接口管理系统访问，它可以无条件关闭，或者通过传递一个挑战/回应序列，采用多种访问模式开启。

运行时完整性检测器支持定期检查预先定义的存储器区域，通过持续计算和对比这些存储器区域的哈希函数，检查是否存在（有害或缺陷代码）修改情况。

使用外部篡改检测引脚可以检测设备的物理攻击状况。

最后，ARM TrustZone还支持将系统分隔为安全区域和非安全区域，控制这些区域之间的访问特权。

安全监控器会采集所有的安全故障，并且评估它们的严重程度，这是安全非易失存储单元的一部分，然后会执行各自相应的操作。这可以是自动删除敏感信息，例如密钥，并且通知操作系统这种违规。

与安全相关的第二个模块便是加密引擎模块，它涵盖了实施安全和加密算法的加速。注意，这是预引导加载器使用的功能，旨在加速解密/验证引导过程。这个模块为IPSec、SSL/TLS、WiMAX和各种其它标准相关的算法提供硬件加速功能；其中许多功能涉及到了单次传递处理，无论物联网(IoT)的数据何时必须经由设备进行交换与传输。这是一种模块化和可扩展的安全内核，经过优化可以处理所有任务，甚至采用单次传递的数据执行多算法操作（例如3DESHMAC-SHA-1）。在硬件中实施的部分算法包括XOR、DES、AES和NIST认证的随机数生成器。

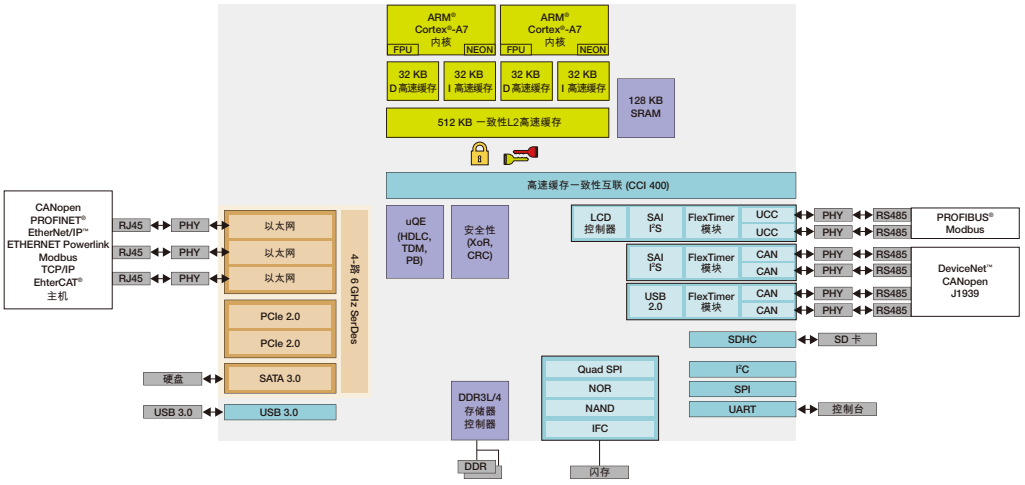
总结

为了支持工业控制、M2M和物联网(IoT)应用的高性能、高度安全的网络连接性，必须满足某些基本要求：出色的可靠性、确保数据安全，交付高效的包处理，并且增强连接性支持。QorIQ LS1021A处理器的设计可以满足这些要求，交付出色的性能效率，可以提供连接性和安全功能的优化组合。

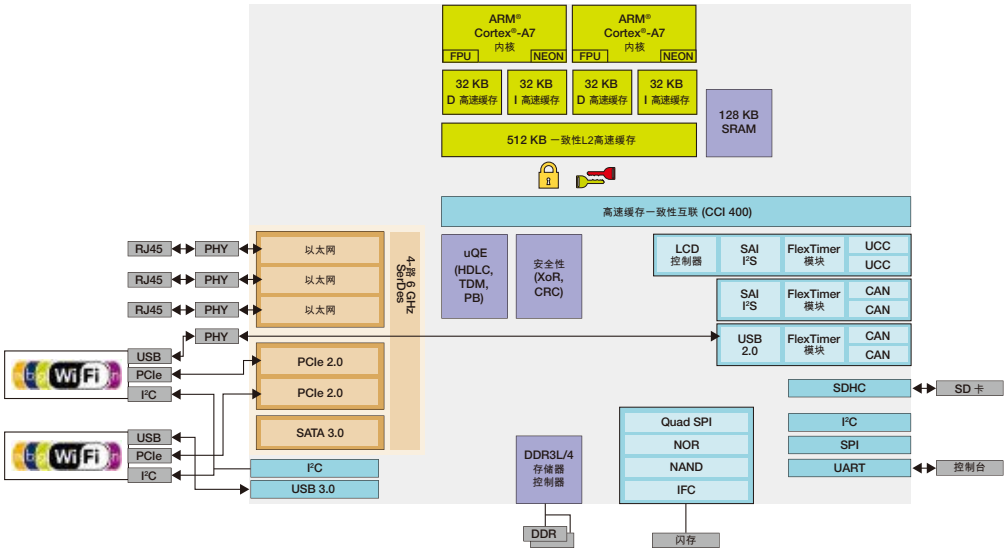
实例应用

以下是工业和物联网(IoT)应用的实例使用案例集合，它们都是基于QorIQ S1021A处理器获得支持。

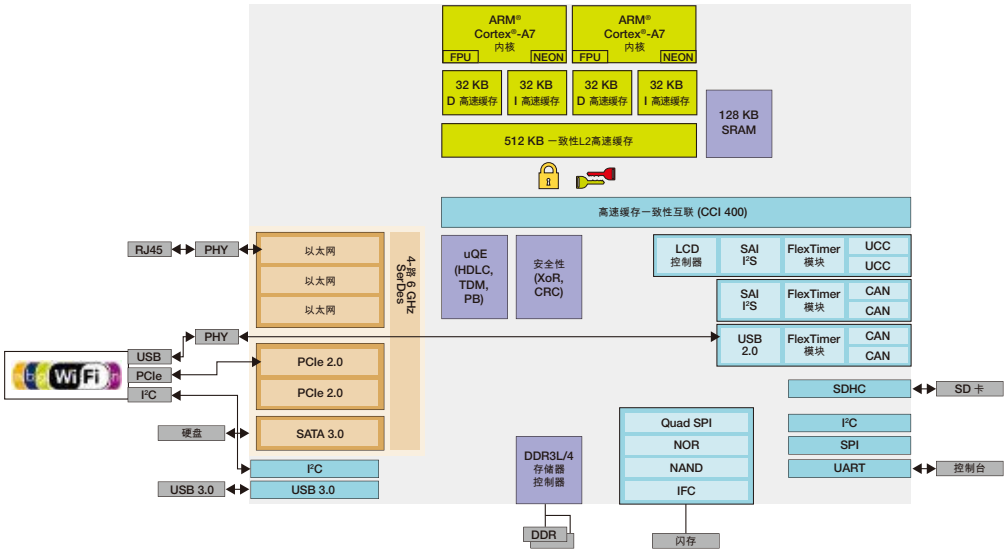
可编程逻辑控制器(PLC)：QorIQ LS1021A处理器



无线网关（可信节点）： QorIQ LS1021A处理器



网络连接加密存储：QorIQ LS1021A处理器



欲了解更多信息，敬请访问以下网址：freescale.com/QorIQ

文档编号：QORIQINDIOTWP REV 0
2014年8月