White Paper

High-Performance, Highly Secure Networking for Industrial and IoT Applications

Abstract

The networking, industrial control, Machine-to-Machine (M2M) and emerging Internet of Things (IoT) markets all share a similar basic requirement: the ability to safely and securely connect a variety of end points and support centralized control across the network. The widespread adoption of the Internet Protocol (IP) standard now commonly used in enterprise networks by the industrial automation, M2M and IoT markets is allowing them to leverage common networking building blocks across these emerging application spaces. This paper will discuss the additional requirements for ensuring industrial, M2M and IoT networks incorporate support for trust, security, high reliability and efficient performance.

Table of Contents

freescale™

Introduction

The networking, industrial control, machine-to-machine (M2M) and emerging Internet of Things (IoT) markets all share a similar basic requirement: the ability to connect a variety of end points together and support centralized control of the network. The widespread adoption of the Internet Protocol (IP) standard enables industrial automation, M2M and IoT applications to leverage common network connectivity building blocks.

The adoption of Ethernet to enable connectivity between machines on the factory floor has been growing steadily as manufacturers seek greater visibility to data, improved productivity and the ability to remotely manage their industrial operations. Enhancing the visibility and management of networked factory devices, which enables streamlining of their associated functions, depends on the ability to ensure the data carried across the factory network remains secure.

Freescale continues to lead the industry in this trend as one of the top suppliers of networking processors used in control and data plane applications for more than 20 years. Whether the design involves networking infrastructure, industrial control networks (gateways or PLCs) or factory floor equipment, some essential requirements must be satisfied: deliver exceptional reliability, data security, efficient packet processing and enhanced connectivity support.

Freescale first established itself as the industry leader for networking solutions by supporting these requirements with its communication processors based on Power Architecture® technology. Building on this expertise and record of innovation achieved over the past twenty years, Freescale announced the first QorIQ networking processor family based on the ARM® ISA. The innovative QorIQ LS1021A processor is equipped with dual high-efficiency ARM Cortex®-A7 cores with ECC-protected L1 and L2 caches to ensure maximum reliability and support operating speeds up to 1 GHz. The dual ARM cores are complimented by the highest level of integration ever offered in a sub-3 W microprocessor. High-performance networking interfaces include Gigabit Ethernet, PCI Express® 2.0, SATA 3.0 and USB 3.0. The LS1021A processor also features support for legacy serial interfaces, including TDM, HDLC, UART, I^2C, SPI, CAN and PWM/Quadric decoding. In addition to the wide variety of communication interfaces, the processor offers support for SDHC, I^2S, and an integrated LCD controller.

Communication Accelerators

In process automation and manufacturing control applications, the network must be always available, highly reliable and secure. At the same time, network processors need to provide intelligent features that allow companies to take advantage of the flow of information available today within their networks.

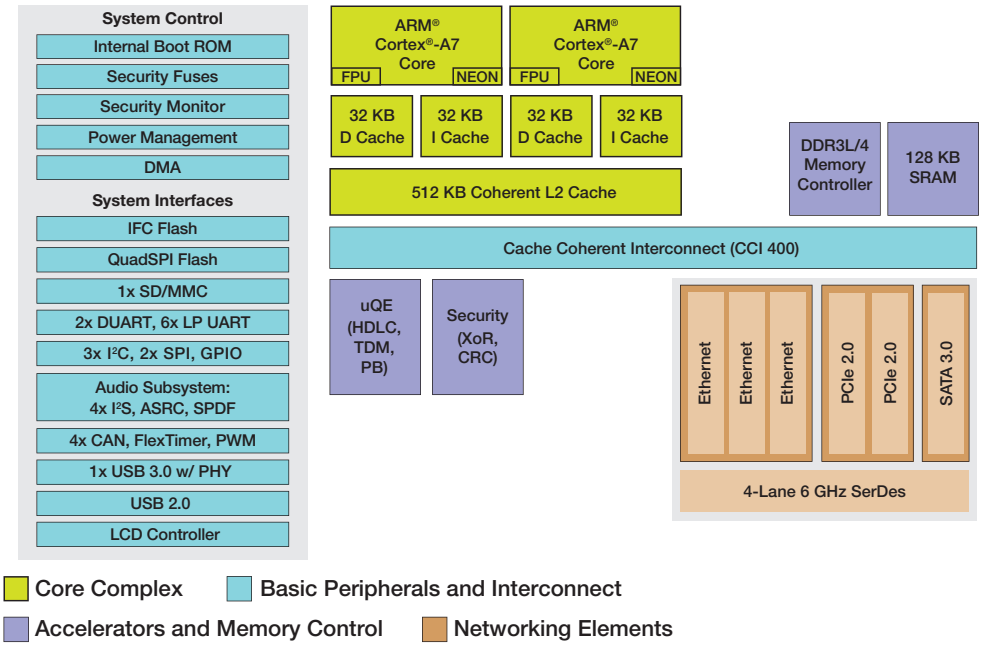
To deliver maximum reliability and bullet-proof security, Freescale network processors integrate industry-leading network acceleration and protection technologies. Among these technologies is the programmable micro QUICC Engine that supports Field Bus and RS485 protocols such as PROFIBUS (both master and slave), as well as legacy HDLC and TDM communication protocols.

Supporting Ethernet connectivity, each of the virtualized, enhanced triple speed Ethernet controllers (VeTSEC) support IEEE® 1588 time stamping on both ingress and egress, along with timer and pulse implementation in hardware. The hardware also supports software

managed queues, which when combined with the ingress parsing up to ISO layer 4 and hardware prioritization on egress, allows for simple effective queuing to be implemented.

These proven Ethernet controllers are common to other Freescale processors used in industrial applications and are supported by a wide variety of mature software drivers, including software stacks for Industrial Ethernet (EtherCAT® Master), PROFINET® (RT), EtherNet/IP™ and PRP.

QorIQ LS1021A Processor Block Diagram



Enterprise Network Lineage Features

The QorIQ LS1021A processor was designed from the ground up to meet the needs of demanding and rugged networked applications. This is achieved by incorporating error detection and correction (ECC) technology on all memories, including Layer 1 and 2 caches, as well as SRAM and external DDR memory for maximum reliability, as well as watchdog timers. Complimenting the reliability enabled by ECC-protected memories is a high-performance security engine that supports a full array of data protection mechanisms, including secure boot, trust architecture, ARM TrustZone® and manufacturing protection, which together enable the maximum in trusted node capability.

These features are essential in IoT applications where many edge of network devices and sensors will be capturing and transmitting user-specific data between nodes. Since this data can be directly related or linked to an individual user, it is essential that the data be encrypted. This is increasingly being regulated and monitored by legislation which extends to the specification of encryption standards and protocols to be used. The inevitable result will be a requirement that communication processors used in M2M or IoT applications must have the capability of performing cryptographic operations, such as hashing, signing and encrypting data, as well as a secure key storage unit in order to meet regulatory requirements.

Industrial communication links must also be secure, not just from data snooping but also from unauthorized control which could result in such costly events as taking down a production line.

However, even if the data transmitted between the network communication links is encrypted, the physical device may still be vulnerable to attack via an unauthorized modification of the program software. Therefore, a device must not only provide secure communication, but be able to operate as a trusted node. A trusted node is a device that the user can fully rely on to not only protect data, but to ensure it only executes authentic software created for it by the user.

In the real world trust is typically conferred, and this concept extends in similar fashion to the digital world. If you get information (data or a command) from a trusted source, you can assume that it is reliable, valid information. Booting up a trusted device requires a “root of trust,” which can be an external (typically expensive) device, such as an FPGA or ASIC, or it can be integrated in the SoC (system-on-chip) itself, as it is in the QorIQ LS1 product family. In the case of the LS1021A processor, authentication is performed within a preboot loader that is contained completely in internal ROM. This implementation provides a one-time user programmable authentication KEY to be used with the preboot loader, creating the trust needed to prevent unauthorized code/users from manipulating the system. The trusted node feature is enabled by writing the authentication KEYs and an enable bit, which are one-time user programmable fuses. Once the Trust mode is enabled, external boot code image(s) (e.g., boot loader, OS kernels or even bare metal code) will only be executed after it has been decrypted and authenticated by the preboot loader KEYs. This code then becomes the next source of trust. Included in the decrypted/authenticated code can be data-like KEYs that can be used in the trusted communication links. Support for a primary and alternate (secondary) signed code images to provide additional reliability.

The external code image is encrypted using the same KEY(s) blown into KEY area on the QorIQ LS1021A processor by the user’s development team with the tool chain provided to program the device. Hence, the code image is known to be secure when it leaves the development group.

Once the code image is authenticated by the device, the device operates in the “secure” state. To maintain the secure operation state, additional security features are available to detect and prevent unauthorized tampering or manipulation of the code/data in external memory.

The secure debug controller manages access to the system through the JTAG interface, which can be closed down unconditionally or be opened in various access modes upon passing a challenge/response sequence.

The Run-Time integrity checker supports periodic checks of predefined memory regions for modification (by harmful or defective code) by continuously calculating and comparing hashes of these memory regions.

An external tamper detection pin can be used to detect physical attacks to the device.

Finally, ARM TrustZone supports the division of the system into secure and nonsecure zones and controls access privileges between those zones.

All security failures are collected and their severity evaluated by the security monitor that is part of the secure nonvolatile storage unit, which then executes the respective actions. This could be the automatic deletion of sensitive information, such as KEYs, and to notify the operating system of such a violation.

The second block related to security is the cryptographic engine block, which covers acceleration of the security and encryption algorithms to be implemented. Note, this is used by the preboot loader to accelerate the decryption/authentication boot process. This block provides hardware acceleration for the algorithms associated with IPSec, SSL/TLS, WiMAX and various other standards; many of them with single-pass processing involved whenever data in the IoT has to be exchanged and transported out of the device. It is a modular and scalable security core that is optimized to process all it can, and even perform multi-algorithmic operations (e.g., 3DESHMAC-SHA-1) in a single pass of data. Some of the algorithms implemented in hardware are XOR, DES, AES and a NIST-certified random number generator.

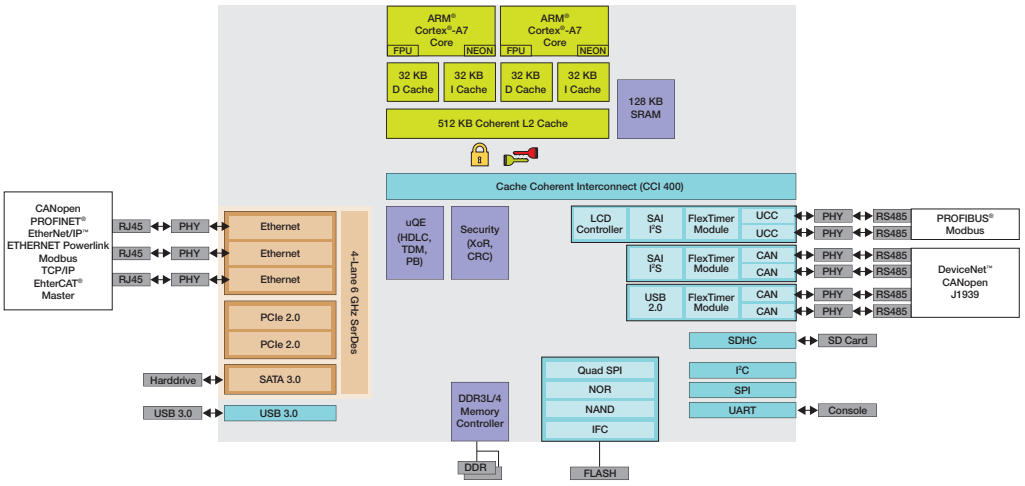
Summary

To enable high performance, highly secure network connectivity for industrial control, M2M and IoT applications, some essential requirements must be satisfied: exceptional reliability, ensure data is secure, deliver efficient packet processing, and enhanced connectivity support. The QorIQ LS1021A processor has been engineered to meet these requirements, delivering exceptional performance efficiency together with an optimized mix of connectivity and security features.

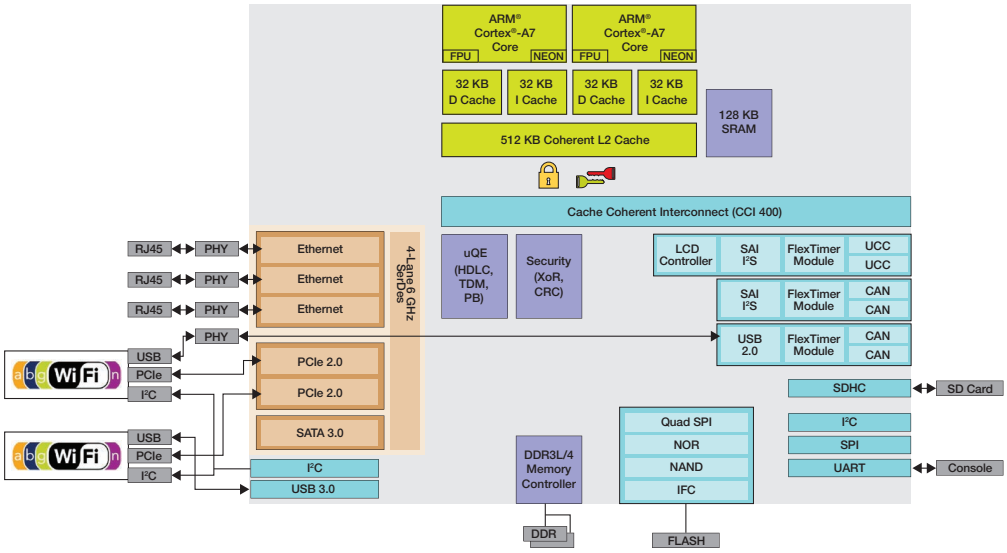
Example applications

Following are a collection of example use cases for industrial and IoT applications that can be supported based on the feature set of the QorIQ S1021A processor.

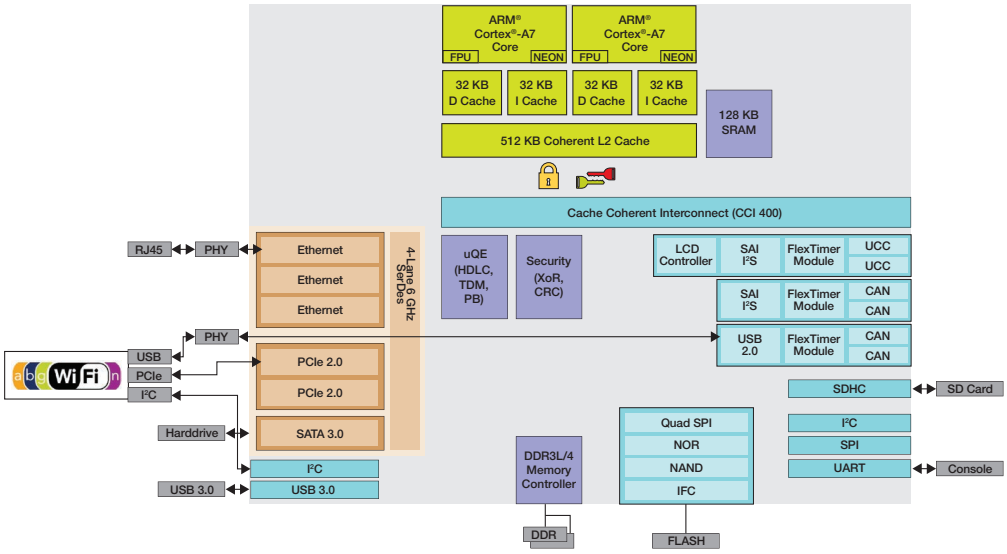
Programmable Logic Controller (PLC): QorIQ LS1021A Processor



Wireless Gateway (Trusted Node): QorIQ LS1021A Processor



Network Attached Encrypted Storage: QorIQ LS1021A Processor



For more information, please visit freescale.com/QorIQ

Document Number: QORIQINDIOTWP REV 0

August 2014