Gateway Implementations with RISC-V

Alex Pluemer for Mouser Electronics

(Source: a-image - shutterstock.com)

MOUSER ELECTRONICS

Reduced instruction-set architectures (ISAs) such as RISC-V provide greater efficiency and less drag on resources than their more complex counterparts. Industrial Internet of Things (IIoT) applications often require both high connectivity and cooperation levels between modules while keeping costs down and reducing power consumption. The Terasic T-Core FPGA MAX 10 Development Board provides a comprehensive hardware design platform built around the Intel® MAX 10 FPGA for RISC-V-based designs. It's an optimal development solution for cost-effective designs in control plane or data path applications and features industry-leading programmable logic for design flexibility.

Gateways in IIoT Applications

An Internet of Things (IoT) gateway combines and bridges a variety of sensor readings—often using analog, digital, or simple serial communications—to higher-level serial communications channels such as a simple UART, more complex channels like I2C or SSI, or even CAN, USB, or Ethernet. This bridge often does some local computation so that raw data doesn't need to be sent to the cloud—instead, a notification is sent when a sensor reading moves out of range.

A development platform for such an IoT bridge requires a significant amount of flexibility—on the sensor side supporting a variety of analog inputs, general purpose inputs, and simple serial communications; and on the management side providing higher level communications (such as I2C, and SSI)—while providing computational and storage capability for data processing.

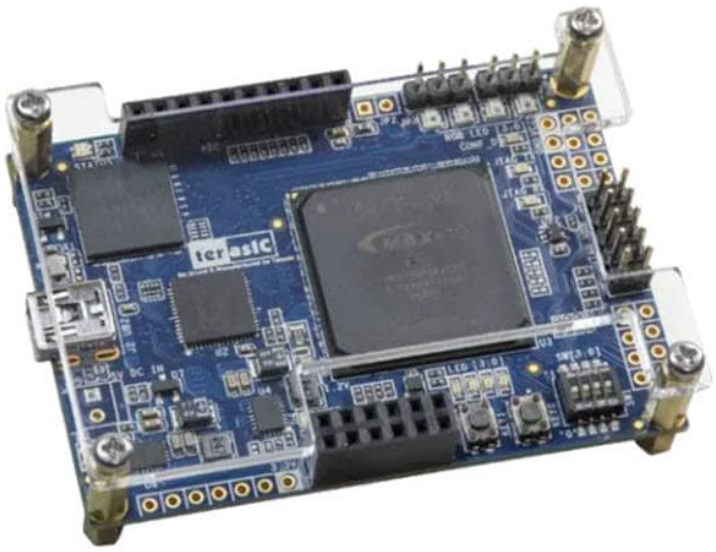

Figure 1: LThe T-Core FPGA MAX 10 Development Board (Source: T-Core FPGA MAX 10 Development Board - Terasic Technologies | Mouser)

An ideal target development board for this type of bridge is the Terasic Technologies T-Core FPGA MAX 10 Development board **(Figure 1)**.

The MAX 10 FPGA can implement many standard serial interfaces programmable logic elements. The FPGA can also host a RISC-V core for processing, and the board has an off board QSPI flash device for source code and data storage. The FPGA has dual ADCs, with up to 10 pins for sensor readings. The board has 12 I/O pins for either general purpose use or use as I2C or SSI communications channels.

Implementing RISC-V for Bridging Applications on the Terasic T-Core FPGA MAX 10 Development Board

Implementing the efficient RISC-V processor on the development board directly aligns with many of the key requirements of an IoT bridge. The most critical aspects include increased efficiency in power and processing, lower costs, wide protocol flexibility, and strong security.

Efficiency

One of the fundamental advantages of the RISC-V ISA is its processing efficiency. Simple CPU operations use memory directly without specialized processor registers, increasing speed and reducing the required memory footprint. With a cache subsystem, frequently used locations are automatically available with reduced access times—reaping the benefits of fast specialized register access without complicated and less efficient coding. Gateways benefit from this advantage with low power and small code space. Also, gateways are very data-transfer intensive because data packets are typically only transferred, broken down, or stitched together. Minimal processing is needed to change from one protocol to another, making efficient memory movement a key benefit. More efficient processing also helps implement AI-oriented gateway functions to identify unusual events and predict potential issues before they become problems.

Flexibility and Protocol Support

Gateways need to be flexible at the protocol, operating system, and in physical connectivity, and modular in construction. The RISC-V open-source architecture makes it easy to support various protocols and adapt to changing requirements. Accessing the source code for peripheral drivers and stacks and the associated protocols makes it easy to modify them as needed, both during development and even after deployment. This makes it easy to modularize peripherals and protocols so they can be easily swapped, updated, or enhanced as industry standards change. This can extend an IIoT gateway's lifetime and reduce the overall system deployment cost–a key factor in IIoT implementations.

Security

RISC-V hardware-based security is needed to implement the root of trust, the bedrock of any robust security system. The root of trust is the known secure starting point for a host of security-related functions such as secure boot, cryptographic computations, secure key, and certificate storage. The root of trust is commonly supported with specialized hardware for protecting secured data and peripheral functions, implementing tamper protection, generating keys, and providing secure

updates to application software. When a system requires cloud storage, the gateway can use trusted cryptographic standards to protect data to and from the cloud **(Figure 2)**. With open-source implementations available for encryption, decryption, certificate management, and secure data communication protocols, the developer has access to all the security-related code, making it easier to test and verify the design's robustness. Additionally, the ability to customize and upgrade the code as needed for specific application requirements—without the need to wait for a third party to develop and release periodic updates—is an additional benefit of an open-source environment.

Conclusion

Gateways will continue to evolve as the IIoT environment produces new applications and revenue streams. As they change and become more complex, additional processing power will be required, meaning more data processing within the gateway to minimize data traffic to the cloud will also be needed. The Terasic T-Core FPGA MAX 10 Development Board can provide developers with the tools they'll need to design cost-effective, single-chip solutions for these data-intensive applications. The out-of-the-box RISC-V support available with the kit is conducive with the efficiency, flexibility, and security required for IoT bridges in the present and future.

Figure 2: The gateway can use trusted cryptographic standards to protect data to and from the cloud.
(Source: sdecoret - shutterstock.com)