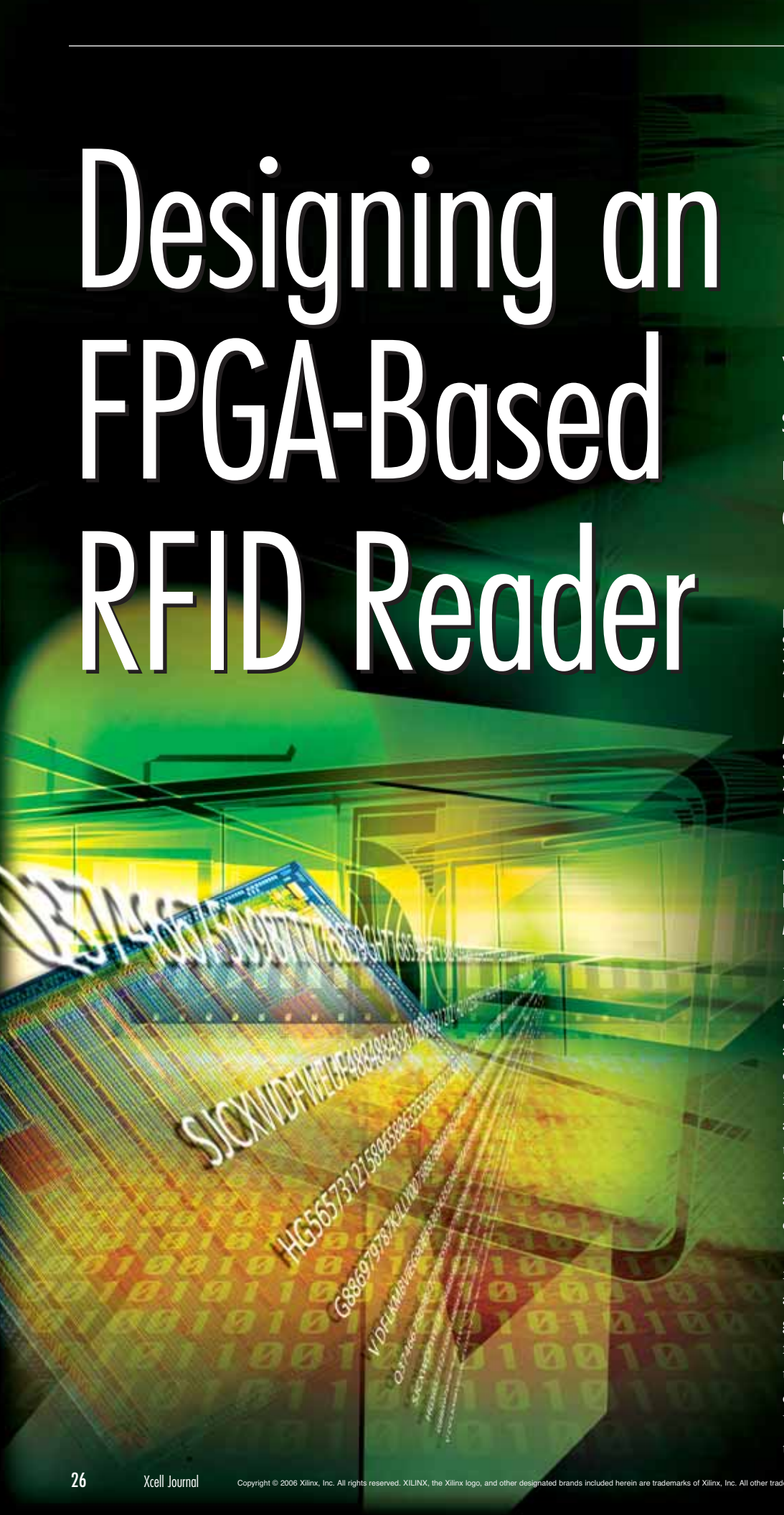
Designing an FPGA-Based RFID Reader



You can implement a practical, standards-compliant RFID reader using off-the-shelf RF components and FPGAs.

by Niladri Roy
Sr. Manager – ISM, Vertical Marketing
Xilinx, Inc.
niladri.roy@xilinx.com

Akshaya Trivedi
Sr. Systems Architect – Wireless, Vertical Marketing
Xilinx, Inc.
akshaya.trivedi@xilinx.com

James Wong
Product Marketing Manager
Linear Technology Corp.
jwong@linear.com

Radio-frequency identification (RFID) is an auto-identification technology similar to other common auto-ID technologies such as bar codes or magnetic strips. A physical object is associated with a unique identifying number (UID) that is incorporated in an RFID transponder, or "tag." The tag is usually attached to a physical object, such as a carton, a pallet, or a container filled with a product. An RFID reader (interrogator) extracts the UID from the tag.

A basic RFID system has three components: an antenna or coil, a transceiver with a RFID decoder, and an RFID tag programmed with the UID. Table 1 shows the four commonly used RFID frequencies and their potential applications. The frequency of greatest commercial interest at this time is UHF, with potentially large-volume applications in supply chain management.

	Frequency	Distance	Example Application
LF	125 KHz	Few cm	Auto-Immobilizer
HF	13.56 MHz	1m	Building Access
UHF	900 MHz	~7m	Supply Chain
µwave	2.4 GHz	10m	Traffic Toll

Table1 – RFID frequencies

EPC Tags

EPC stands for electronic product code, a standard for RFID tags, including both the data content of the tag and the open wireless communication protocols. The EPC movement combines data standards used in bar-code specifications with the wireless data communication standards that ANSI and other groups (802.11b) have developed. The EPC standard currently employed in supply-chain management is EPC Class 1 Gen II.

Class 1 tags are nominally factory programmed, but could be field downloadable. Normally, once the tag is written to, the memory is locked and further write operations disallowed. Class 1 tags use a conventional packet-oriented protocol, with the reader transmitting a packet containing commands and data, followed by a response from the tag.

Hostile Reader Environments

RFID system environments can be quite hostile. The frequency channels operate in a license-free ISM (industrial, scientific, and medical) band. RFID readers in this band are prone to external interference from cordless telephones, wireless headsets, wireless data networks, and other co-located readers. Each reader's RF receiver front end must be designed to withstand high-interference signal levels without introducing distortion products that cause interrogation errors. The receiver noise needs to be low so that it has sufficient dynamic range to allow error-free detection of low-level responding tag signals.

The reader RF transceiver architecture shown in Figure 1 is a proven design that works well in such dense, hostile environments. Both the transmitter and receiver incorporate a high dynamic range direct conversion modulator and demodulator, respectively, for maximum robustness and minimum cost.

A Practical Robust RF Receiver Design

The heart of the receiver is built around Linear Technology's LT5516, a highly integrated direct conversion quadrature demodulator with an on-chip precision quadrature phase (0° and 90°) shifter. The signal from the antenna, after passing through an RF filter, is fed directly into the demodulator inputs through a balun transformer. Because the noise figure of the LT5516 is low, an LNA (low noise amplifier) is not required, preserving its 21.5 dBm IIP3 and 9.7 dB P1dB performance.

During the receive cycle, the reader transmits a continuous wave (un-modulated) carrier to power the tag. When queried, the tag responds with a bitstream by amplitude modulating the carrier. The modulation format is ASK (amplitude shift key) or PR-ASK (phase-reversal ASK). The demodulator has two quadrature phase-detected outputs that provide an inherent diversity receive function. If one path receives no signal because of a multipath or phase cancellation, the other path (which is 90° phase shifted) would receive a strong signal, and vice versa. As a result, overall receiver robustness improves.

Once demodulated, you can AC-couple the I (in phase) and Q (quadrature phase) differential outputs to an op amp configured as a differential amplifier converted to a single-ended output. You should set the high-pass corner at 5 kHz – below the minimum signal content of the receive data stream and above the maximum Doppler frequency that may be introduced by a moving tag, while still well above the 60 Hz power-line frequency. The resulting outputs can then pass through a low-pass filter pair using the LT1568 configured as a fourth-order low pass. You should set the low-pass corner to a frequency of 5 MHz, allowing the maximum bitstream signal to pass through to the baseband.

The baseband signal can now be digitized by a dual, low-power analog-to-digital converter, the LTC2291, which has 12 bits of resolution. Because the tag bitstream has a bandwidth ranging from 5 kHz to 5 MHz, the LTC2291 provides ample oversampling at a rate of 25 MSps, accurately capturing the demodulated signal. If needed, you can implement additional digital filtering in the baseband DSP. This affords maximum flexibility for the receiver to set the logic threshold, which the baseband processor can perform digitally.

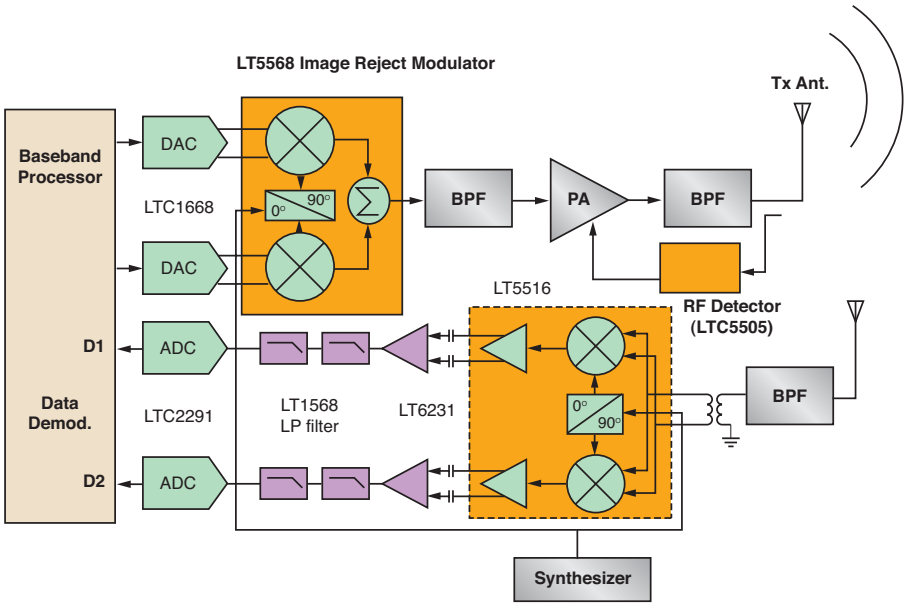


Figure 1 – A practical high-performance RFID transceiver architecture

The baseband tasks and digital RF channelization processing make an all-FPGA solution quite attractive and integrated.

A High Dynamic Range RF Transmitter Design

The transmitter employs an integrated image-reject direct conversion modulator. The LT5568 offers very high linearity and a low noise floor, providing exceptional dynamic range for the transmitted signals. The modulator accepts the baseband I and Q signals in quadrature from digital-to-analog (DAC) converters and modulates directly to the 900 MHz transmit frequency.

Internally, the LO (local oscillator) is split by a precision quadrature phase shifter. The modulated RF signals are combined to create a single-ended, single-sideband RF output with its image suppressed by 46 dBc. Moreover, the modulator has matching I and Q mixers to maximize the suppression of the LO carrier signal to -43 dBm.

The composite modulator circuit exhibits exceptional ACPR (adjacent channel power ratio) performance that helps to meet the transmit spectral mask required. For example, at a modulator RF output level of -8 dBm, the ACPR is better than -60 dBc. With its clean output, the signal can be amplified up to the maximum allowable power of 1W (+30 dBm in the U.S.) or as high as 2W for European compliance. In either case, it is important to maintain this fixed level, as it is used to power the tag and to maximize the reading range. The LTC5505 RF power detector's internal temperature compensation accurately measures the power and provides stable feedback to regulate the RF power amplifier output.

Baseband Processing and Network Interfaces

At the baseband, the FPGA performs channelization of the waveform to the DAC and from the analog-to-digital converter (ADC). This process, also called digital IF processing, will involve some filtering, gain control, frequency translation, and sample-rate change. The FPGA can even process multiple channels in parallel.

Figure 2 shows the partitioning of a potential RFID reader architecture. Other baseband processing tasks would include:

- Preamble detection
- Sequence estimation
- Modulation and demodulation (ASK, frequency and phase-shift keying)
- Signal generation
- Correlator processing
- Peak detection and thresholding
- CRC and checksum
- Encoding and decoding (NRZ, Manchester, unipolar, differential biphase, Miller)
- Frame detection
- ID descrambling
- Security crypto engines

This received RFID tag data is transmitted either over a serial port or a network interface to a corporate enterprise system server.

This traditional architecture is evolving to become part of a sophisticated distributed TCP/IP network, in which the reader will take on the management of its neighborhood tags. The reader now acts as a gateway between a tag and an intelligent distributed database system connected to enterprise software applications.

These baseband tasks could be realized on an FPGA or a DSP – or a combination of the two – based on hardware/software partitioning. Xilinx has a suite of IP cores in the form of FIR, CIC, DDS, DUC, DDC, bit correlators, and sine/cosine LUTs. The logic is well suited to perform crypto engines that use shift registers and XORs. The DSP48 engines for the Xilinx® Virtex™-4 family are well suited to perform other signal processing tasks.

A baseband processor controls the functionality and scheduling of the various baseband tasks; it is responsible for the link-layer protocols as well. These baseband tasks would include frequency-hopping, listen-before-transmit, and anti-collision algorithm processing. The baseband processor could also offer interfaces such as Ethernet, USB, or Firewire.

The baseband tasks and the digital RF channelization processing make an all-FPGA solution quite attractive and integrated. The FPGA functionality, DSP functionality, and baseband processor functionality could all be collapsed into an

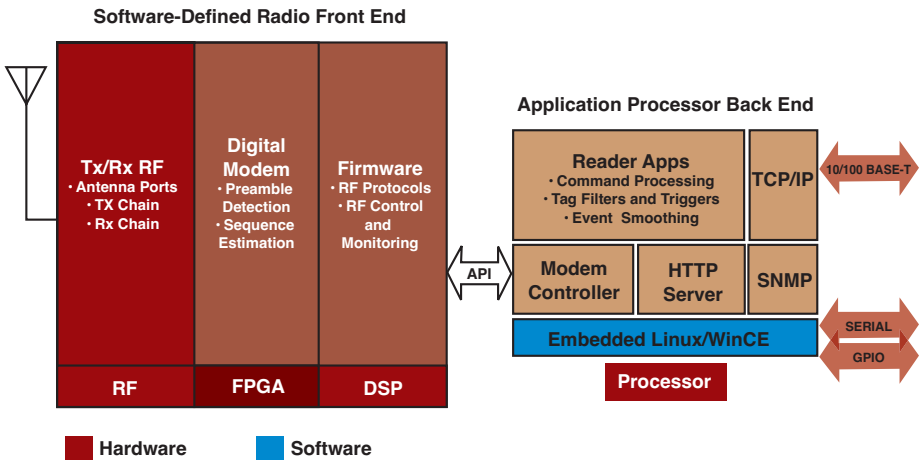


Figure 2 – Potential RFID reader architecture

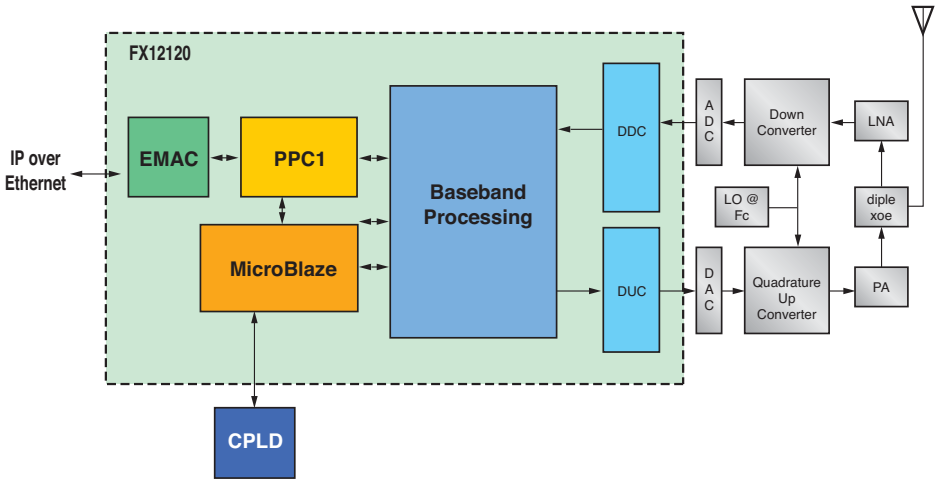


Figure 3 – Virtex-4 FX-based RFID architecture

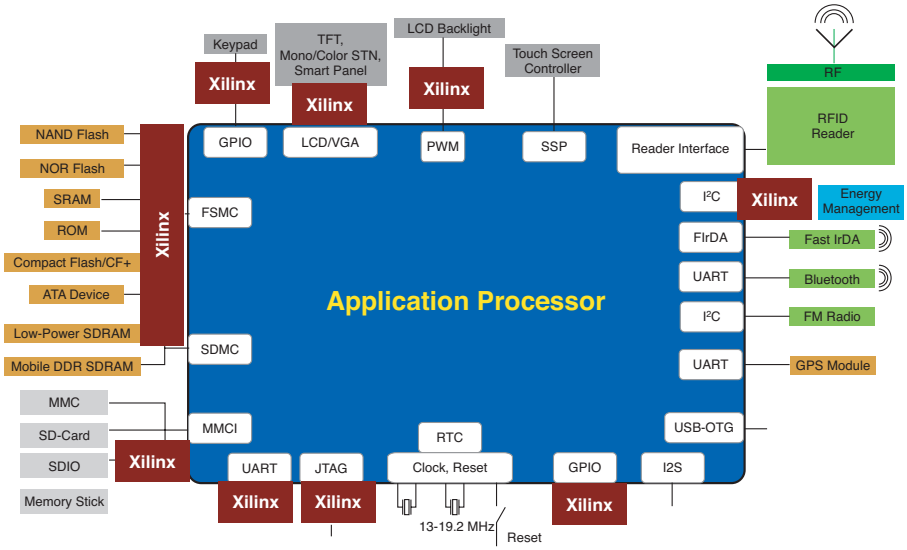


Figure 4 – CoolRunner-II CPLD in RFID readers

FPGA with an embedded processor.

Figure 3 illustrates the potential architecture of an FPGA-based RFID processor. The embedded processor could be a hard IP, like the Power PC™ in the case of the Virtex-4 FX family; it could be a soft-core MicroBlaze™ in Spartan™ devices; or even a PowerPC and MicroBlaze combination. You can connect the built-in hard Ethernet MACs (EMACs) to an external Ethernet PHY to connect to the Ethernet network. As an alternative, you can use Lite Ethernet MAC IP for 10/100-BaseT as well.

The Power PC/MicroBlaze embedded processors perform the following tasks:

- EPC data handling and forwarding
- Protocol handling
- Interrogator scheduling
- TCP/IP network interfacing
- Control and monitoring
- Modem controller
- Upgrade agent
- HTTP server
- SNMP/ MIB handling

The Xilinx Gigabit Ethernet System Reference Design (GSRD) is an EDK-based reference system geared toward high-performance bridging between TCP/IP-based protocols and user data interfaces. The components of the GSRD contain features to address the per-byte and per-packet overheads of a TCP/IP system.

TCP transmit performance benchmarks are available for Monta Vista Linux and Treck stacks. Nucleus PLUS RTOS using the Xilinx Platform Studio (XPS) microprocessor library definition (MLD) brings a new dimension to systems using MicroBlaze and PowerPC processors. Its small size means that it can use available on-chip memory to minimize power dissipation and deliver increased performance, while the extensively available middleware makes it ideal for RFID back-end networking.

Handheld readers can interface to hard disk drives, QWERTY keypads, removable memory interfaces, various display devices, and other peripherals using Xilinx CoolRunner™-II CPLDs, as shown in Figure 4. These CPLDs can also assist the application processor and address these features with little incremental power consumption, high-speed performance, and a small chip package.

Conclusion

Going forward, RFID readers are likely to see front-end DSP functions like RF protocol processing – performed today in discrete DSP – integrated into the FPGA. Embedded soft-processor cores already provide significant DMIPS/MHz performance, and enhanced versions will soon replace back-end external processors for controlling reader applications, providing maximum flexibility and cost reductions for RFID reader equipment through programmable logic.

Xilinx is committed to providing continually enhanced DSP and embedded processing functionality in FPGAs through continuously improved XtremeDSP™ and MicroBlaze configurable soft-processor core offerings.