A Low-Cost Software-Defined UHF RFID Reader with Active Transmit Leakage Cancellation

Edward A. Keehr
Superlative Semiconductor LLC, Carlsbad, CA, United States of America
Email: keehr@super-semi.com

***Abstract*—A monostatic UHF RFID reader targeting personal applications based on recently introduced commercial-off-the-shelf (COTS) software-defined radio (SDR) application-specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs) is proposed. The result is an RFID reader architecture whose principal components cost less than half of those of existing readers, but is flexible as a result of the programmable nature of the FPGA. The reader implements all mandatory EPC Gen 2 commands (except kill) and can perform inventory, targeted programming, blank tag programming, and single-tag analysis via a smartphone interface. The proposed RFID reader architecture adaptively cancels the large CW transmit signal using a reflected power canceller (RPC). The RPC is terminated by a novel subranging tunable microwave network comprising digitally tunable capacitors capable of attenuating transmit leakage at the receiver by over 50dB. The reader achieves -73dBm of sensitivity at the antenna port when attached to a channel model and connectorized tag and achieves an open area tag read range of 2.6m with a 1.2dBi dipole antenna and 15.2m with a 12.5dBi patch antenna.**

I. Introduction

With the utility of RFID for the purpose of tracking and managing everyday objects readily apparent, it is somewhat curious that this technology has not become pervasive in the home and personal electronics markets. Perhaps one major reason for this is the relatively high cost of typical UHF RFID reader modules, which range from $200 to $300 [1]. Part of the reason that RFID readers are so expensive is because the reader application-specific integrated circuits (ASICs) are so expensive. For example, the $23.60 ST Micro ST25RU3980 is the lowest cost reader ASIC available from major distributor websites [2], and even its low price is an outlier. Furthermore, it has the limitation of being able to execute only a single tag read every 500ms [3]. As the primary market for RFID readers remains the deep-pocketed retail sector and sales volumes of reader ASICs remains sized to that market, there is little incentive for new or existing entrants to develop lower-cost ASIC solutions.

An opportunity to explore lower-cost markets without incurring the high cost and risk of RF/Analog ASIC development has arisen over the past few years as a result of three converging trends in electronic design. The first of these trends is the advent of single-chip SDR systems. Recently, low-cost sub-GHz SDR ASICs have been introduced and marketed as "I/Q Transceivers" that currently retail on major distributor websites for about $4 in quantities of 3,000. For this project, the Semtech SX1257 [4] will be utilized due to its low cost and full-duplex capability.

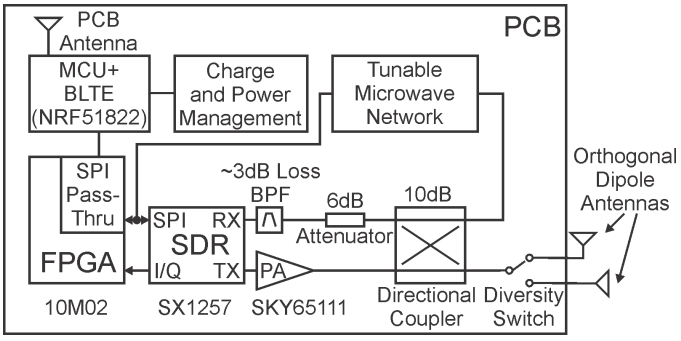

Fig. 1: Proposed Reader PCB Top level Architecture.

In mid-2014, Lattice Semiconductor introduced the iCE40Ultra family of low-cost FPGAs [5] which contain 2,000-3,500 LEs selling for around $4 on Digi-Key in quantities of 4,000. Altera followed this second trend by introducing the 2,304 LE MAX10M02 FPGA family [6], which will be used in this project, selling for as low as $2.84 in bulk. It is the assertion and the topic of this paper, that such FPGAs are large enough to accommodate a fully-functional, albeit feature-limited, RFID reader transceiver digital back end compatible with an SDR ASIC provided that efficient digital design techniques are used.

Designing a RFID reader system with a standard SDR ASIC does have one notable complication. Since an RFID reader transmits a CW signal at up to 1W during reception of the tag backscatter signal, the RFID radio receive chain must process this large TX signal concurrently with the weak RX backscatter signal. Custom RFID reader ASICs may utilize on-chip structures to remove the TX leakage in such a way that the resulting RX performance is still acceptable [7]. Since techniques such as those in [7] are not available in the SX1257, it is therefore proposed to cancel the TX signal externally using a reflected power canceller (RPC) approach similar to that proposed in [8]. The paper in [9] proposed building the tunable microwave network (TMN) of the RPC for an RFID reader with a relatively new class of device (the third trend referred to above) known as a digitally tunable capacitor (DTC), supplied by companies such as WiSpry and Peregrine Semiconductor. However, [9] only provides TX cancellation of 20-30dB for an antenna reflection coefficient of

2573-7635 ©2018 IEEE. Digital Object Identifier 10.1109/RFID.2018.8376193.

-18dB (indicating a high-quality antenna). This performance is insufficient for TX cancellation in a RFID reader based on the aforementioned SDR ASICs. To solve this problem, a TMN topology that enables a reduction in TX leakage of up to 50-60dB for an antenna reflection coefficient of -10dB (a more realistic number for a low-cost antenna) was developed along with a compatible tuning algorithm and is presented in detail in [10]. This new TMN topology uses 4 DTCs from Peregrine selling for $0.65 apiece in quantities of 3,000 on Digi-Key.

In total, the cost of active components required to replace the >$23.60 RFID reader ASIC comes out to about $9.40 in quantities of about 3,000, more than halving of the cost of even the cheapest publicly priced RFID chip. Assuming a BOM-to-retail markup of 5x [11], this means that RFID readers designed using SDRs, FPGAs, and DTCs could fall below the $99 retail price threshold even with the other required components added in, provided that the FPGA implementation can be crafted to support a low-cost MCU or DSP for protocol handling.

II. Prior Art in SDR RFID Readers

Utilizing FPGA-based SDRs to implement UHF RFID transceivers is not a new idea. For example, soon after the first draft of the GS1 EPCglobal "Gen2" air interface protocol in 2004, a magazine article [12] appeared on how to design such a system using discrete radio and data converter components and a Xilinx Virtex-4 FPGA, but neither reported the building nor the performance of said design. Throughout the literature, perhaps the most popular method of implementing an FPGA-based SDR RFID reader is do to so with either the Ettus USRP1 [13] [14] [15] or one of the second-generation USRP platforms [16] [17] [18]. These systems are physically quite large with the former, along with its daughtercards, retailing for $970 or more, and the latter retailing for over $1600. In most of the aforementioned cases, custom design on the onboard FPGA was largely forgone, with the bulk of the EPC Gen 2 signal processing being implemented in GnuRadio and strict protocol timing requirements being met mainly through clever networking and host computer modifications.

Full custom MCU- and DSP-based SDR readers have been described in [19] and [20]. The former addressed the high cost of previous software-defined RFID readers by designing a system with a sub-$40 bill-of-materials ($7 for just the transmitter, receiver, and TX/RX coupler, and $2.30 for standalone MSP430F5510); however, the range of this system was only about 0.15m and its envelope-detecting method of demodulation leaves the design vulnerable to large interfering signals in the license-free bands in which RFID operates. The latter described a system tailored to perform multisine excitation of RFID tags. While the precise BOM of this implementation was not provided, tallying the lowest-cost components called out in the design using the lowest publicly available prices resulted in an active component BOM cost of slightly greater than $40 (minus the PA and transmit cancellation network). While also achieving a lower cost than a USRP platform, this implementation was physically large, did not implement automatic tuning of the transmit cancellation network, and only implemented one EPC operation (Query with Q=0).

SDR reader designs that implement and describe significant portions of the design on FPGA include [21], [22](with [23] [24]), [25], [26](with [27]), and [16](with [28]). These designs all utilize relatively large and expensive FPGAs and radio sections. One exception with respect to the radio is [25], which used an AS3992 reader ASIC (cost: still relatively high at $40 each for 500) only as an RF/Analog front end to implement an RFID listener (RX only, no TX). Furthermore, these designs implement protocol handling using a either a softcore MCU/CPU, which drives up the size of the FPGA due to a higher required resource count, or an external high-speed MCU/CPU/DSP which is likewise expensive and requires a correspondingly higher-speed and higher-cost FPGA to quickly handle protocol traffic in the middle of an EPC Gen 2 transaction. By implementing a small subset of the RFID protocol on the FPGA, the design in [26] addresses this latter point somewhat, but still utilizes a 200MHz Samsung S3C2410 ARM9 processor (cost: not publicly available, but similar 200MHz ARM920T chips cost over $12 in bulk on Digi-Key) to handle the rest of the protocol.

FPGA resource counts for the complete designs of the aforementioned references were not given except for [21], which only described the receiver. Resource counts for FM0-only synchronization and decoding were provided in [23] and [29], the latter of which was referenced in [25] and reported to have been improved upon (but resource count of [25] was not provided). In general, the aforementioned designs use computationally intensive correlator-bank strategies for clock and data recovery, while [29] describes an FM0-specific symbol-by-symbol duty-cycle computing strategy. A summary of all of these works compared to the proposed architecture is shown in Table I. It is important to note that in Table I, only the cost of the SDR, digital baseband, MCU/CPU/DSP, and TX leakage cancellation is tabulated, while items such as the PA, power management, and non-critical passives are ignored.

III. Top Level Architecture

A. Overview

The RFID reader architecture proposed here is shown in Fig. 1. It is controlled by a $2.31 Nordic NRF51822QFAA ARM Cortex M0 MCU connected via Bluetooth low-energy connection to a smartphone running application software. Comparable devices without Bluetooth LE functionality can be had for half the price. The MCU accesses the FPGA via a serial peripheral interface (SPI) bus, and also accesses the SDR ASIC through an SPI bridge in the FPGA. This bridge is required since the TMN tuning algorithm must have access to the SDR gain control registers during radio operation. In principle, over-the-air programming of the FPGA can be performed by the Bluetooth-connected MCU, as it is also connected to the programming interface of the FPGA, although this feature has not yet been implemented. As described in Section I, TX cancellation is achieved by using a DTC-actuated TMN connected to the isolation port of a directional

References	Key Components	SDR BOM Cost	# FPGA LEs	Range	Output Power	Comments
[12]	Assorted LTC Components Xilinx Virtex 4 FPGA USRP1	> $235	> 13824	Not reported	Not reported	No meas. results reported.
[13] [14] [15]	EP1C12Q240C8 FPGA RFX900 x1/x2	>$970	12060	Up to 6-7m [13] [14]	27dBm [13]	Bistatic. 8dBic antennas [13].
[16] [28]	USRP-2922 Spartan-3A DSP 3400 FPGA SBX Card	>$3092	>53714	"Same as AS3992 Eval. Board"	Not reported	Monostatic. Uses dir. coupler to sep. TX and RX.
[17]	USRP-2942 Kintex 7 410T FPGA	>$7373	>406000	>2.35m	Not reported	Bistatic.
[18]	USRP N200 Spartan-3A DSP 1800 FPGA SBX Card	>$2203	>37440	Not reported	17.8dBm	Bistatic. 7dBic antennas.
[19]	TH72035 MAX931 MSP430F5510 MCU	>$ 9	N/A (MCU)	0.15m	9dBm	Monostatic. Dipole antenna (1-2dBi). Not fully tested.
[21]	Stratix II EP2S60 FPGA Big MCU Board Big Radio Boards	>$874	60440	6m	Not reported	RX dig. only described. Antenna config. unclear.
[20]	F28377D MCU ADF4360-3(?) PLL LT5516 Demod(?)	>$40	N/A (MCU)	Not reported	Not reported	Physically Large Manual Tx Cancellation. Only implements Query=0 transaction.
[22] [23] [24]	Various RF Xilinx Virtex II FPGA TI TMS320C6416 DSP	> $500	Up to 93184	11m (in hall)	35dBm	Monostatic. 5dBi antenna.
[25]	AS3992 RF FE XC3S500 FPGA	$73.55	10476	3.5m	N/A	Receiver only. "Loop antenna".
[26] [27]	Various RF Virtex 4 LX100 FPGA S3C2410 MCU	>$2500	>110592	8-9m	30dBm	Antenna gain or config. not reported.
Proposed	SX1257 SDR MAX 10M02 FPGA 2x PE64102, 2x PE64906 NRF51822QFAA MCU	$ 11.71	2304	2.6m (dipole) 15.2m (patch)	26dBm	Monostatic. Dipole (1.2dBi) and patch (12.5dBi) antennas measured. 64cm^2 Board Area. Goal: 7m dipole range.

TABLE I: Summary of prior art in SDR/FPGA - based RFID readers.

coupler in an RPC configuration. A diversity switch connected to two antenna ports, both in monostatic configuration, is included.

B. Select System Calculations

In this section, a set of key calculations is performed to assess the transmit cancellation requirements assuming the use of the SX1257 SDR ASIC and a 7m tag read range with a dipole antenna. While the actual design did not quite meet these targets, the exercise is still instructive to relate as it translates the characteristics of the SDR ASIC to specifications on the remainder of the system.

1) Expected RX Signal at Antenna at 7m Range: Assume that there exists +29dBm TX PA output power (P_{TX}=29dBm) (slightly under 1W as per USA FCC regulations), the use of a lossy reader dipole antenna with 1dBi gain G_{READER}=1dB, the use of a tag dipole antenna with 1dBi gain G_{TAG}=1dB, that the reader has one antenna with polarization close to that of the tag, and transmission of an RFID reader signal at 915MHz in free space. Using the Friis transmission equation $P_{RX} = P_{TX} + G_{READER} + G_{TAG} + 20\log 10(\frac{\lambda}{4\pi R})$ one can compute that for R=7m, the tag receives -17.6dBm of RF power, which is sufficient to excite a typical RFID tag [30] for reading. The tag backscatter loss of a tag such as [30] can be expressed as $10\log 10(\alpha|\Delta\Gamma|^2)$ where α=0.25 [31] and $|\Delta\Gamma|$=0.8 [30] and results in a value of 8dB. With the transmission gain from the tag back to the reader equal to $G_{READER} + G_{TAG} + 20\log 10(\frac{\lambda}{4\pi R})$ = -46.6dB, the total tag power returned is -17.6dBm-8dB-46.6dB = -72.2dBm. This number represents the required reader sensitivity.

2) Required Cancellation Ratio of TX Leakage: There are two limitations setting the required TX leakage cancellation ratio prior to the SDR ASIC. One is that the residual phase noise needs to be far enough below the RX signal to permit the acquisition and decoding of the latter. The second is that both the RX signal and any remaining downconverted TX leakage at DC must both pass through the SX1257 ADCs without the former saturating the ADC while the latter is significantly above the ADC noise floor. In order to correlate TX and RX phase noise terms $\phi_{TX}(t)$ and $\phi_{RX}(t)$ as much as possible, the SDR ASIC PLL bandwidths are extended to their maximum of 300kHz. In this case, phase noise at the BLF of 187.5kHz is in principle dominated by that of the crystal reference shared between the TX and RX PLLs. As such, $\phi_{TX}(t)$ and $\phi_{RX}(t)$ are expected to be highly correlated. If this were perfectly true, the RX baseband phase noise would be zero. This result seems rather optimistic, however, and it will be assumed rather that a more modest 3dB improvement in phase noise is obtained than if $\phi_{TX}(t)$ and $\phi_{RX}(t)$ were perfectly *un*correlated. The phase noise term referred to the receiver input can then be expressed as $A_{TX}(\phi_{TX}(t))$ assuming similar $\phi_{TX}(t)$ and $\phi_{RX}(t)$.

Based on [4], the SSB phase noise of the SX1257 can be estimated to be -101dBc/Hz at 187.5kHz. The TX amplitude is +29dBm at the antenna and the 3dB bandwidth of the RX digital bandpass channel filter is 90kHz. Combining these quantities as +29dBm +10$\log_{10}$(90000Hz) -101dBc/Hz +3dB (to account for SSB to DSB conversion) yields a total antenna-referred phase noise of -19.5dBm prior to TX cancellation rel-

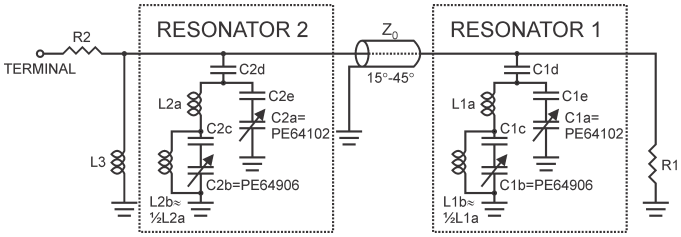

Fig. 2: Proposed Tunable Microwave Network Circuit.

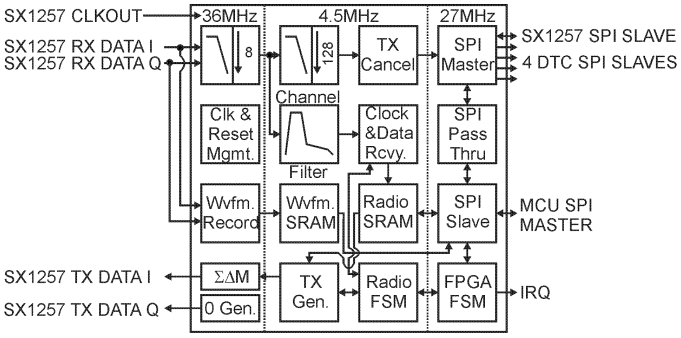

Fig. 3: FPGA Top level Architecture.

ative to a minimum RX backscatter signal power of -72.2dBm at the antenna. Hence, a TX cancellation of about 50dB (plus the 10dB reduction in returned signal power afforded by the -10dB reflection coefficient of the antenna) is required to achieve a baseband SNR of 7dB for proper clock recovery and decoding of the tag backscatter signal. With this level of TX cancellation, the antenna-referred baseband DC signal arising from TX leakage is -31dBm, which easily fits within the 13-bit (72dB) dynamic range of the SX1257 ADCs during reception of a -72.2dBm antenna-referred RX signal. Also with this level of TX cancellation, the residual phase noise referred to the SX1257 input is -19.5dBm-10dB(antenna S11)-50dB(cancellation)-19dB(front end losses)=-98.5dBm. This number can be compared to the measured SDR ASIC input-referred phase noise performance in [10].

IV. Tunable Microwave Network

The proposed TMN for the SDR RFID reader is depicted in Fig. 2. The architecture is a coupled resonator topology [32] modified with inductive transformers which are used to create subranging tunable capacitors (C1b, C2b) to increase the reflection coefficient coverage density in a clean and collinear (with C1a and C2a) manner. The worst-case achievable cancellation ratio (not including the -10dB assumed antenna reflection coefficient) is found to be 50dB. More details regarding this network, its characterization, adaptive tuning algorithm, and performance can be found in [10].

V. FPGA Digital Back End

A. MCU Interface

The proposed FPGA top level block diagram is shown in Fig. 3. The FPGA is driven by the MCU through the SPI interfaces

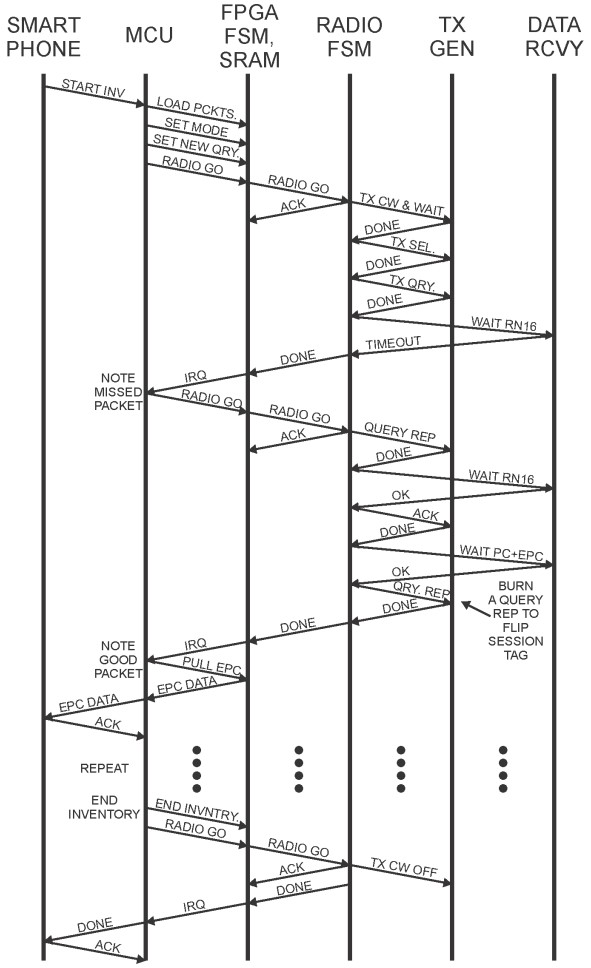

Fig. 4: Exemplary Inventory Operation with MCU and FPGA.

shown on the right hand side. For a given operation (e.g. inventory, program), the MCU loads the Radio SRAM with the packet information required for the transmit operations. Once this is done, the MCU kicks off one of several RFID EPC Gen 2 operations by selecting the appropriate operation then by sending the 'RADIO GO' command via SPI write to the FPGA. After a transaction is complete, the MCU may read out its results from the Radio SRAM via SPI. An example inventory operation depicting protocol signaling throughout the SW/HW stack is shown in Fig. 4. In this implementation, EPC information is pulled from the reader to the smartphone at every successful tag PC+EPC extraction in the inventory. Due to the long delay involved with the Bluetooth transfer, the Radio FSM must issue a dummy Query Rep in order to flip the tag's inventory flag prior to handling off control back to the MCU. While shuttling data in this manner prolongs the actual RFID operation relative to storing the tag EPC information locally on the FPGA, the total time required to perform the inventory and extract all of the tags' EPC data over Bluetooth would be roughly the same.

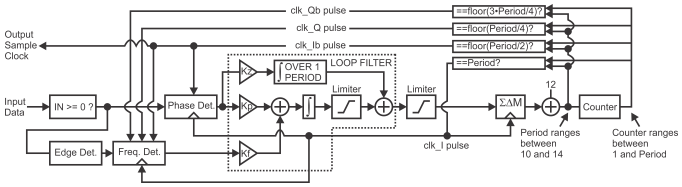

Fig. 5: Representation of clock recovery circuit.

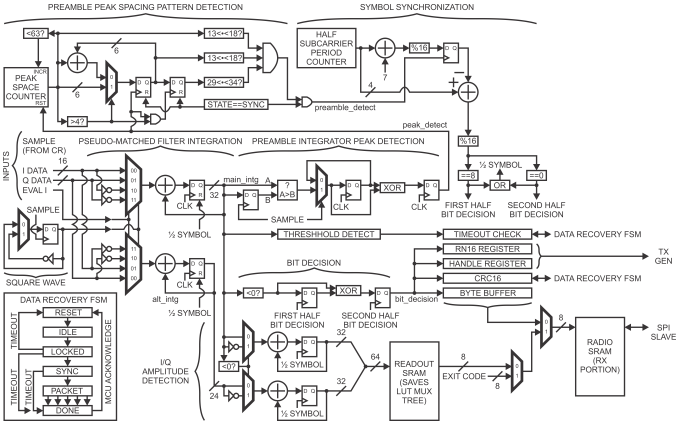

Fig. 6: Representation of data recovery block.

B. Receiver

In order to maximize the signal-to-noise ratio of the receiver, the choice was made to fix the mode of operation to Miller, M=8 with backscatter link frequency (BLF)=187.5kHz. This choice permits long matched filter integration times while keeping the tag signaling frequency far away from lower frequencies dominated by SX1257 phase noise.

1) Filtering: The filtering portions of the FPGA are shown in the upper left section of Fig. 3. From the left hand side, the 36MHz clock and RX data are provided by the SX1257 SDR. The RX data is first filtered and decimated by a factor of 8 so that it can be processed in a more efficient fashion by the rest of the DSP blocks. This decimated data is bandpass filtered using two cascaded direct-form II biquadratic filters with center frequencies straddling 187.5kHz and with a composite 3dB bandwidth of 90kHz to support the +/-12.5% allowed variation in BLF in both I and Q channels. The outputs of these latter filters go on to the CDR circuitry. The outputs of the decimate-by-8 filters also go on to decimate-by-128 filters, again in both I and Q channels, that supply an estimate of the residual TX leakage to the adaptive TX cancellation algorithm driving the TMN. The decimate-by-128 filters are each a cascade of a first-order IIR filter and an integrate-and-dump filter, a more resource-efficient combination than a second-order IIR filter.

2) Clock Recovery: A representation of the digital PLL-based clock recovery (CR) circuit is shown in Fig. 5. At any given time, it operates on only the I or Q input signal. At 126 4-input LUT/49 flip-flops, it consumes vastly less resources than the smallest reported approach [23] (660 4-input LUT/1398 flip-flops) in prior FPGA-based SDR UHF RFID literature and can in principle work for both Miller and FM0 signaling. A digital PLL-based timing recovery loop intended for a UHF RFID receiver has been previously reported in [33]. The circuit in [33] consumes 1151 LUT, 364 flip-flops, and 3 multipliers on an FPGA. In order to handle the 22% required lock-in range, the design uses a BLF pre-estimator circuit to reduce the loop lock-in range to 8%. It requires a piecewise parabolic interpolator and uses an NCO (counter) with "fractional" interval but does not say how the fractional interval is achieved. Timing error detection in [33] utilizes a Gardner circuit [34] which utilizes full-bitwidth adders and multipliers and thereby imposes relatively large bitwidth requirements on the loop filter.

By contrast, the CR design in Fig. 5 calculates timing error using a hybrid phase detector/rotational frequency detector scheme [35] which only uses 11 4-LUT and 12 flip-flops and only outputs +/-1 and +/-2 values to the loop filter, keeping its required resources low. Such a scheme natively permits a frequency lock-in range of +/-25% [36] and has no inherent need for a pre-estimator circuit or a parabolic interpolator in the context of UHF RFID. "Fractional" NCO (counter) intervals are accomplished by dithering the 3-bit NCO control input with a low-complexity first-order sigma-delta modulator to improve PLL stability [37].

3) Data Recovery: A detailed depiction of the data recovery (DR) block is shown in Fig. 6. Pseudo-matched-filtering is performed using a correlate-and-integrate-and-dump scheme on each incoming half symbol. Bit decisions are performed on only the I or Q input signal at any given time by comparing two half-symbol results. While this incurs a 3dB SNR penalty against a true MF bit decision, it was found that the CR performance dictates sensitivity anyway. Symbol timing recovery is performed during the preamble by the peak detection, peak spacing detection, and symbol synchronization circuits in Fig. 6. The symbol timing recovery process is also aided by the same correlate-and-integrate circuit used later for bit decisions. These circuits are required for Miller signaling, since symbol boundaries cannot be trivially determined by examining half-BLF-intervals as in FM0. So when comparing resource counts to FM0-only designs such as [21] [23] [25] [29], it would not be appropriate to include this circuit. The design in [33] "focuses on FM0 code for common use" and only provides test results for FM0, so will be likewise assumed to have an FM0-only symbol synchronizer. The peak spacing pattern detection circuit counts the number of half-BLF intervals between integrator output peaks and looks for a 32-16-16 pattern to detect a preamble. Spurious peaks due to noise are filtered out by stalling the peak spacing pattern detector FIFO when peak spacings below a certain value are detected. The DR block also contains circuitry to compute I and Q magnitude for offline phase difference of

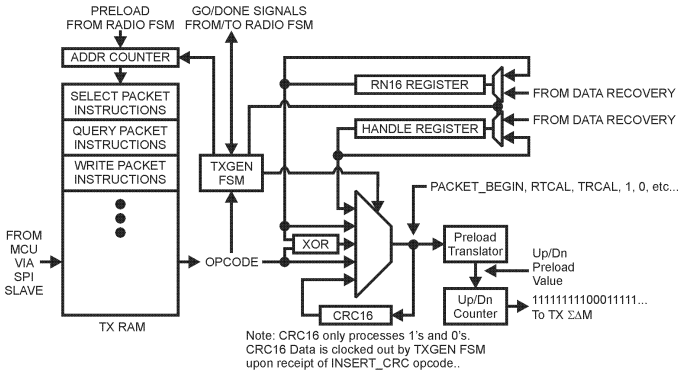

Fig. 7: Representation of TX baseband waveform generator.

arrival (PDOA) [38] analysis, to multiplex various data to SRAM, and to perform some local protocol operations such as bit counting, timeout detection, and CRC.

4) Waveform Capture: About halfway down the left side of Fig. 3 is the waveform record block. Eight KB of raw SDR RX data at a programmable time offset from 'RADIO GO' assertion can be stored to Waveform SRAM for offline signal processing to permit advanced tag localization techniques. This operation is currently disabled to save about 60 4-LUT.

C. Transmitter

1) TX Baseband Waveform Generator (TX GEN): The TX baseband waveform generator (TX GEN) is an opcode-driven FSM, depicted in Fig. 7, which controls an up-down counter that ultimately generates an DSB-ASK waveform at RF. For example, a 'RTCAL' opcode causes the counter, running at 4.5MHz, to count high 222 times (49.3us) and low 42 times (9.3us). The FSM reads 4-bit opcodes, shown in Table II, from a segmented SRAM in which each segment corresponds to a particular packet type, such as Select, Query, or Lock. Each time a change is required to a packet, for example to change the Query Q, the MCU must rewrite the corresponding segment of the SRAM prior to recommencing radio operations. To the best of the knowledge of this author, such an opcode-based transmit scheme has not been described as part of an SDR/FPGA-based UHF RFID reader. It permits all of the operations in the RFID transaction to be stored locally on the FPGA, permitting a slow, cheap MCU to preprogram the FPGA over SPI and then let the FPGA handle the remainder of the operation.

2) Sigma-Delta Modulator: The TX GEN block is followed by a third-order ΣΔM similar to that prescribed for use in [4]. Inside, DC offset compensation for the SX1257 I input is implemented in order to achieve the ASK modulation depths required by [39]. The SX1257 Q input is driven by a high/low counter called "0 Gen" whose high/low count pattern is designed to generate harmonics at the null frequencies of the digital FIR filter within the SX1257 and to provide DC offset compensation. The aforementioned offset values are

Opcode	Value	Explanation
TXCW	0000	TX CW Tone for 1.8ms.
BEGIN SELECT	0001	Begin a select packet.
BEGIN REGULAR	0010	Begin a regular packet.
DUMMY ZERO	0011	Insert a zero, don't count it in CRC.
SINGLE ZERO	0100	Insert a zero, count towards CRC.
SINGLE ONE	0101	Insert a one, count towards CRC.
RTCAL	0110	Insert RTCAL.
TRCAL	0111	Insert TRCAL.
NAK END	1000	Provides short TX CW time after NAK.
XOR NEXT 16b	1001	XOR next 16b with RN16.
INSERT CRC	1010	Insert CRC.
INSERT RN16	1011	Insert RN16.
INSERT HANDLE	1100	Insert Handle.
LAST WRITE	1101	Break write loop in Radio FSM.
END PACKET	1110	Return control to Radio FSM.
BEGIN IMMED	1111	Begin an immediate response packet.

TABLE II: TX GEN Opcodes

Block	4-LUT	FF	LE	9x9 Mult.	RAM Bits
RX Filters	569	437	631	16	0
Clock Recovery	126	49	129	0	0
DR-PMF & Bit Decis.	50	33	50	0	0
DR-Symbol Sync.	117	61	117	0	0
DR-I/Q Magnitudes	160	88	160	0	0
DR-SRAM Muxing	68	8	68	0	128
DR-Local Protocol	86	81	86	0	0
DR-Total	499	286	499	0	128
Radio FSM	137	17	142	0	0
SPI	199	146	218	0	0
TX Cancel	222	118	222	16	8192
TX Gen	210	71	211	0	0
TX ΣΔM	159	82	160	0	0
Others	35	37	69	0	8320
Total	2156	1320	2281	32	16,512
Limit	2304	2304	2304	32	110,592

TABLE III: FPGA Resource Allotment

programmed into the FPGA flash memory, similar to how a production ASIC trim memory might be flash-programmed.

D. Reader Limitations

In order to reduce the number of required FPGA resources, several compromises were made to the receiver design. First, TX Tari is fixed to 46.875kHz, while backscatter communications are fixed to Miller, M=8, at a nominal BLF of 187.5kHz. Second, clock and data recovery (CDR) can only proceed for either I or Q data at any given time. The effect of this second limitation is that the effective read rate is slowed as both I and Q data need to be checked. Similar compromises were made in the design of the ST25RU3980 [3] [40], so these items are not considered to be significant limitations to this design. Since the proposed reader targets a personal/home application, tight digital transmit filters for multi-/dense-reader emissions masks are neither required nor included. The current design targets operation in the 902-928MHz band with 500kHz wide channels. The current design also requests a long pilot from the tag to ensure CR acquisition and does not specially handle collisions. The current design has not yet been tested with frequency hopping, but is believed to work with only software modifications. Finally, as discussed earlier, the design makes sub-optimal bit decisions and utilizes only DSB-ASK TX.

VI. Implementation Details

The realized RFID reader is shown in Fig. 8. The board measures 188.5mm by 34mm. From left to right, the board

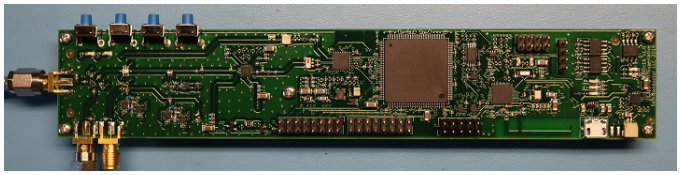

Fig. 8: Proposed Software-Defined RFID Reader.

contains RF circuitry, digital circuitry, and PMU circuitry. Of note is that the FPGA utilized for the demonstration is not the cheapest available in the Altera 10M02 family. The FPGA utilized was a 10M02SCE144A7G due to part availability limitations at the time of board manufacture. The 144-EQFP package was utilized due to the difficulty and expense of manufacturing and assembling with the cheapest 10M02DCV36C8G 36-WLCSP package. The FPGA design was successfully compiled for the 10M02DCV36C8G (including meeting timing requirements) and the 10M02SCE144A7G configuration image actually uses only the ASIC pins available on the lowest cost 10M02DCV36C8G. Therefore, it is expected that the FPGA design utilized in this paper can be utilized immediately on a $2.84 FPGA. The board is powered by a 5V USB-Micro-B connector receptacle.

The antennas utilized by the reader for this demonstration were 1.2dBi gain dipoles with better than -10dB reflection coefficient from 902-928MHz. These antennas were separated from the PCB by 6" of coax cable to reduce self-interference to the board. The firmware written for this demonstration reader is verified to be capable of conducting four operations: searching for a specific tag, inventory, programming a blank tag, and programming of a specific tag. Along with the FPGA code, it implements all of the mandatory commands of [39] except for Kill, although this can be trivially added with a few extra FPGA LE and MCU software additions.

FPGA resource usage is shown in Table III. Note that each LE consists of a 4-input LUT and a flip-flop. Register packing is used extensively to close the design.

VII. Measurement Results

A. Output Power

The output power of the reader was measured at 26dBm with a power meter. While the reader is capable of transmitting 29dBm, harmonic distortion from the diversity switch making its way back into the receiver prevents proper TMN operation at these levels. In a future revision, applying a higher control voltage to the switch is expected to solve this problem.

B. Example TX Waveform and Modulation Depth

An exemplary reader-tag exchange is captured over the air and shown in Fig. 9. Modulation depth from build to build has been observed to be 18dB or greater after SX1257 offset calibration in the FPGA is performed.

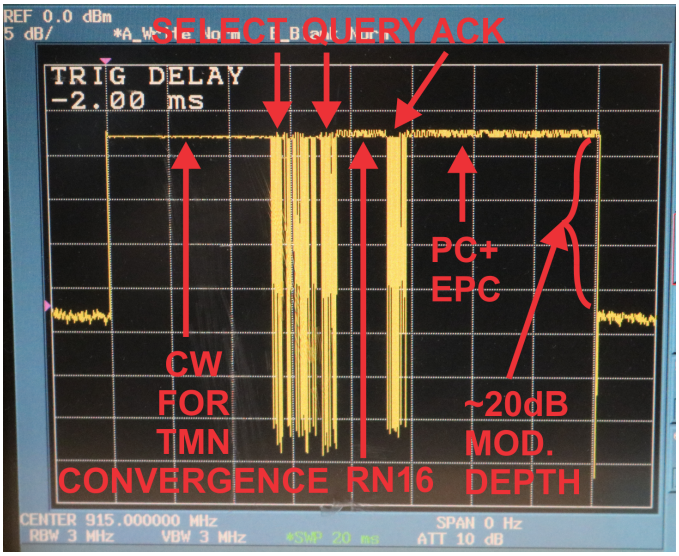

Fig. 9: Exemplary Over-the-Air Reader-Tag Exchange showing Modulation Depth.

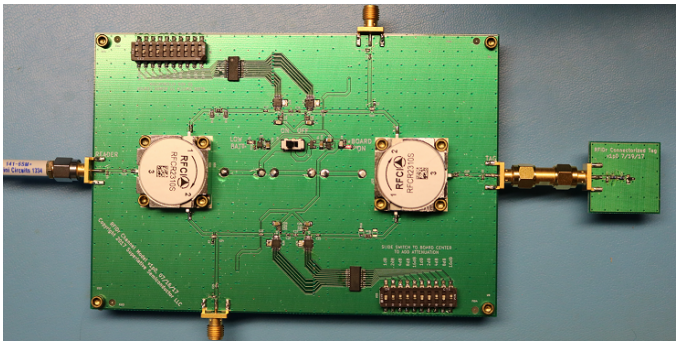

Fig. 10: Channel Model and Connectorized Tag for Sensitivity Measurement.

C. Sensitivity

The sensitivity of the reader was measured with the aid of a channel model board with variable attenuation and connectorized tag, shown in Fig. 10, as was done in [19]. The forward path attenuation was set such that the power received at the NXP SL3S1002FTB1 tag chip was a few dB above its power-on threshold. Sensitivity was assumed when over 50% of the reads (each read consisting of an I and Q read) resulted in proper EPC+CRC capture. At sensitivity, the round-trip attenuation of the channel model board was measured to be 91dB. The tag backscatter loss could not be easily measured or estimated from the tag chip data sheet, but for the purposes of this experiment is assumed to be 8dB, as in Section III-B. In this case, for an output power of 26dBm, sensitivity is computed to be -73dBm at the antenna port. Note that at this level, actually all reads were received with proper EPC+CRC.

D. Range

The range of the RFID reader was tested in a suburban cul-de-sac with no nearby obstructions. The range test was

performed with an Avery-Dennison 600368 tag featuring a Monza 5 IC. A roughly 50% read (each read consisting of an I and Q read) success rate was achieved at 2.6m away from the tag when the tag is oriented in the same direction as the reader antenna. This range was lower than expected for a number of reasons. First, the reader output power was reduced as discussed in Sec. VII-A. Second, the uncancelled phase noise in the reader increased when an external antenna was used. Tonal behavior in the phase noise was observed during antenna use, suggesting the presence of another coupling path into the SX1257 or its frequency reference. In order to show the usefulness of the proposed reader in an industrial environment, a measured range of 15.2m was also achieved with a 12.5dBi linearly polarized patch antenna.

E. Read Speed (Inventory)

An inventory of 50 Avery-Dennison 600368 tags oriented in the same direction as and positioned about 1.5m away from the reader antenna is taken. All 50 tags could be read in 20 seconds. The limiting factor here is the Bluetooth LE connection between the reader and the smartphone, as was described in Sec. V-A. When an EPC is not detected, Query Reps happen on intervals of about 2ms.

VIII. Conclusion

A complete SDR/FPGA-based UHF RFID reader of lower cost than any yet presented thus far was described in this paper. It is hoped that the reporting of this result spurs the widespread use of RFID in the home and personal markets while at the same-time permitting software-defined field upgrades to match frequent advancements in tag and protocol technologies. Complete FPGA resources were enumerated as a benchmark for further developments in this area.

References

[1] "How much do RFID Readers cost today?" https://www.rfidjournal.com/faq/show?86, accessed: 2017-12-17.

[2] "Digi-Key Electronics," https://www.digikey.com, accessed: 2017-11-22.

[3] *Gen2 - Save Power and Cost: AS3980 - Low Cost UHF Reader IC*, ams AG, Dec. 2013.

[4] *SX1257: Low Power Digital I and Q RF Multi-PHY Mode Transceiver*, Semtech Corp., Feb. 2012, rev. 1.

[5] "Lattice Press Release," http://www.latticesemi.com/About/Newsroom/PressReleases/2014/201407LatticesNewiCE40UltraFamily.aspx, accessed: 2018-02-12.

[6] *MAX10 FPGA Device Architecture*, Altera Corp., May 2015, rev. 2015.05.04.

[7] S. Chiu *et al.*, "A 900 MHz UHF RFID Reader Transceiver IC," *IEEE J. Solid-State Circuits*, vol. 42, pp. 2822–2833, Dec. 2007.

[8] W.-K. Kim *et al.*, "A Passive Circulator for RFID Application with High Isolation using a Directional Coupler," in *Proc. 2006 European Microwave Conference*, Sep. 2006, pp. 196–199.

[9] M. Koller and R. Kung, "Adaptive Carrier Suppression for UHF RFID using Digitally Tunable Capacitors," in *2013 European Microwave Conference*, Oct. 2013, pp. 943–946.

[10] E. A. Keehr, "A Low-Cost, High-Speed, High Resolution, Adaptively Tunable Microwave Network for an SDR UHF RFID Reader Reflected Power Canceller," in *Proc. IEEE Int. Conf. RFID*, Apr. 2018.

[11] "EEVblog Electronics Community Forum: Relationship between Retail price and BOM cost?" https://www.eevblog.com/forum/projects/relationship-between-retail-price-and-bom-cost/, accessed: 2018-02-05.

[12] N. Roy *et al.*, "Designing an FPGA-Based RFID Reader," *Xcell Journal*, vol. 2, pp. 26–29, 2006.

[13] M. Buettner and D. Wetherall, "UW-CSE-09-10-02: A flexible software radio transceiver for UHF RFID experimentation," Univ. of Washington, Tech. Rep., Oct. 2009.

[14] G. Smietanka *et al.*, "Implementation and extension of a GNU-Radio RFID reader," *Adv. in Radio Sci.*, vol. 11, pp. 107–111, July 2013.

[15] L. Catarinucci *et al.*, "A Cost-Effective SDR Platform for Performance Characterization of RFID Tags," *IEEE Trans. Inst. and Meas.*, vol. 61, pp. 903–910, Apr. 2012.

[16] F. Galler, T. Faseth, and H. Arthaber, "SDR based EPC UHF RFID reader DS-SS localization testbed," in *IEEE Wireless and Microwave Technology Conf. (WAMICON)*, Apr. 2015, pp. 1–4.

[17] L. Gortschacher *et al.*, "SDR Based RFID Reader for Passive Tag Localization Using Phase Difference of Arrival Techniques," in *2016 IEEE MTT-S Int. Mic. Symp.*, May 2016, pp. 1–4.

[18] N. Kargas *et al.*, "Fully-Coherent Reader With Commodity SDR for Gen2 FM0 and Computational RFID," *IEEE Wireless Comp. Letters*, vol. 4, pp. 617–620, Dec. 2015.

[19] P. Nikitin *et al.*, "Simple low cost UHF RFID reader," in *Proc. IEEE Int. Conf. RFID*, Apr. 2013, pp. 126–127.

[20] A. J. S. Boaventura *et al.*, "The Design of a High-Performance Multisine RFID Reader," *IEEE Trans. Microwave Theory and Tech*, vol. 65, pp. 3389–3400, Sep. 2017.

[21] C. Huang *et al.*, "A New Architecture of UHF RFID Digital Receiver for SoC Implementation," in *IEEE WCNC*, Mar. 2007, pp. 1659–1663.

[22] C. Angerer *et al.*, "A flexible dual frequency testbed for RFID," in *Proc. 4th Int. Conf. Testbeds and Research Infrastructures for the Development of Networks and Communities*, Mar. 2008, pp. 3:1–3:6.

[23] ——, "Advanced Synchronization and Decoding in RFID Reader Receivers," in *Proc. IEEE RWS*, Jan. 2009, pp. 59–62.

[24] R. Langwieser *et al.*, "A modular UHF reader frontend for a flexible RFID testbed," in *Proc. 2nd Int. EURASIP Workshop on RFID Tech.*, July 2008, pp. 1–12.

[25] A. Borisenko, M. Bolic, and M. Rostamian, "Intercepting UHF RFID signals through synchronous detection," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013:214, pp. 1–10, Aug. 2013.

[26] C. S. Yoon *et al.*, "A Design of UHF-band RFID reader using FPGA," *ResearchGate*, pp. 1–4, Nov. 2014.

[27] C. Jin *et al.*, "A Robust Baseband Demodulator for ISO 18000-6C RFID Reader Systems," *Int. J. Dist. Sensor Networks*, vol. 2012, pp. 1–12, Jul. 2012.

[28] F. Galler, T. Faseth, and H. Arthaber, "Implementation aspects of an SDR based EPC RFID reader testbed," in *Intl. EURASIP Workshop on RFID Tech.*, Oct. 2015, pp. 94–97.

[29] N. F. B. Bautista *et al.*, "Enhanced FM0 Decoder for UHF Passive RFID Readers Using Duty Cycle Estimations," in *Proc. IEEE RFID-TA*, Sep. 2011, pp. 306–312.

[30] *Monza 5 Tag Chip Datasheet*, Impinj, Inc., Aug. 2016, version 3.0.

[31] P. Nikitin and K. Rao, "Antennas and propagation in UHF RFID systems," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 277–288.

[32] R. Whatley *et al.*, "CMOS Based Tunable Matching Networks for Cellular Handset Application," in *Proc. IEEE Intl. Micr. Symp.*, Jun. 2011, pp. 1–4.

[33] P. Wei *et al.*, "Synchronization with Timing Recovery Loop in UHF RFID Reader Receivers," in *Proc. 17th IEEE ICECS*, Dec. 2010, pp. 1148–1151.

[34] F. M. Gardner, "A BPSK/QPSK Timing-Error Detector for Sampled Receivers," *IEEE Trans. Comms.*, vol. 1986, pp. 423–429, May 1986.

[35] L. Devito *et al.*, "A 52 MHz and 155MHz clock-recovery PLL," in *IEEE ISSCC Dig. Tech. Papers*, Feb. 1991, pp. 142–143.

[36] D. G. Messerschmitt, "Frequency Detectors for PLL Acquisition in Timing and Carrier Recovery," *IEEE Trans. Comms.*, vol. 27, pp. 1288–1295, Sep. 1979.

[37] R. B. Stazewski *et al.*, "Digitally Controlled Oscillator (DCO)-based Architecture for RF Frequency Synthesis in a Deep-Submicrometer CMOS Process," *IEEE Trans. Circuit and Systems II*, vol. 50, pp. 815–828, Nov. 2003.

[38] P. Nikitin *et al.*, "Phase based spatial identification of UHF RFID tags," in *Proc. IEEE Int. Conf. RFID*, Apr. 2010, pp. 102–109.

[39] "EPC radio-frequency identity protocols generation-2 UHF RFID specification for air interface protocol for communications at 860MHz - 960MHz version 2.0.1 ratified," 2015.

[40] *UHF RFID Single Chip Reader EPC Class1 Gen2*, ams AG, Jul. 2015, version 1-00 Short Datasheet.