

TRF79xxA NFC/HF RFID Training

Josh Wyatt
TI S2 MCU Division
NFC/RFID Applications
05/2013

TI Wireless Connectivity Portfolio

134KHz/13.56 MHz	Sub 1GHz	2.4GHz			5GHz	Satellite
PaLFI	SimpliciTi	SimpliciTi	ZigBee Pro & IP	Bluetooth	WiFi 802.11 a/b/g/n + Bluetooth	GPS
NFC ISO14443B ISO15693	6LoWPAN	PurePath™ Wireless Audio	6LoWPAN	Bluetooth Low Energy		
	W-MBus		RF4CE	ANT		
Applications						
Medical Point of Sale Smart Energy Electronic Shelf Labeling Access/ Security	Metering Home Automation Electronic Shelf Labeling Alarm & Security	Headphones Gaming Headsets Speakers Human Interface Device & Gaming	Smart Energy Sensor Networks Remote Control Home Automation Healthcare	Mobile Accessories Gaming Controllers Health & Wellness Sports & Fitness	Devices Portable Data Terminals Medical Devices Camera, Video Surveillance Navigation Remote clocking Industrial / Home	
Products						
TMS37157 TRF796x TRF796xA, TRF7964A, TRF7970A	CC1101 CC1110 CC430 CC1120	CC2500 CC2510 CC8520	CC2530 CC2531 CC2533 CC2520	CC2560/7 CC2540 CC2570/1	WL1271/3	CC6000
					WL1281/3	









Denotes TI Proprietary solution or customer defined protocol on these products



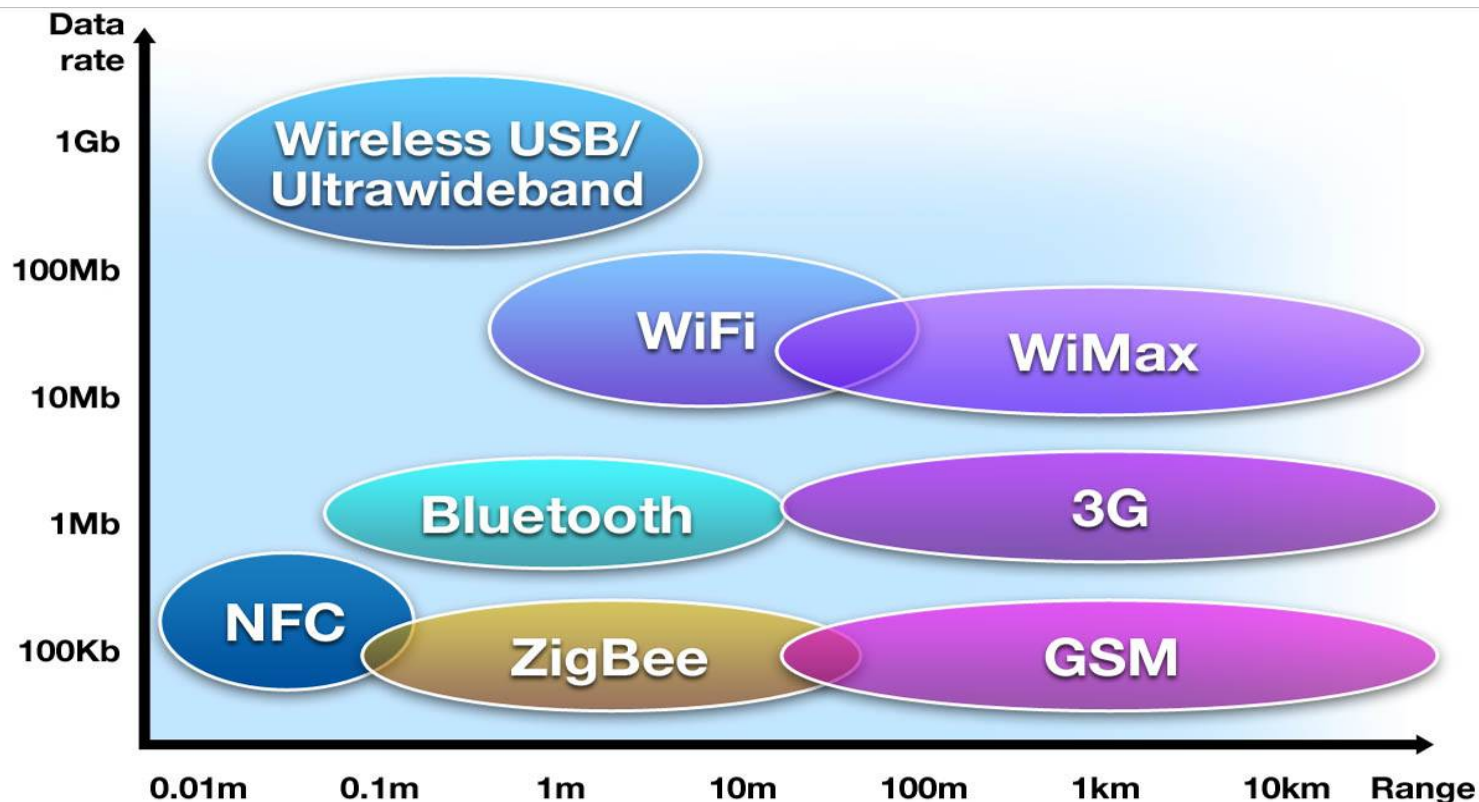
NFC/RFID in Action

NFC/RFID technology has the power to bring new simplicity and convenience to many aspects of a typical person's daily life

	STATION AIRPORT	VEHICLE	OFFICE	STORE RESTAURANT	THEATER STADIUM	ANYWHERE
Area						
Usage of NFC Mobile Phone	Pass gate Get information from smart poster Get information from information kiosk Pay bus/taxi fare	Adjust seat position Open door Pay parking fee	Enter/exit office Exchange business cards Log in to PC; Print using copier machine	Pay by credit card Get loyalty point Get and use coupon Share information and coupon among users	Pass entrance Get event information	Download and personalize application Check usage history Download ticket Lock phone remotely
Service Industries	Mass Transport Advertising	Public Transport	Security	Banking Retail Credit Card	Entertainment	Any

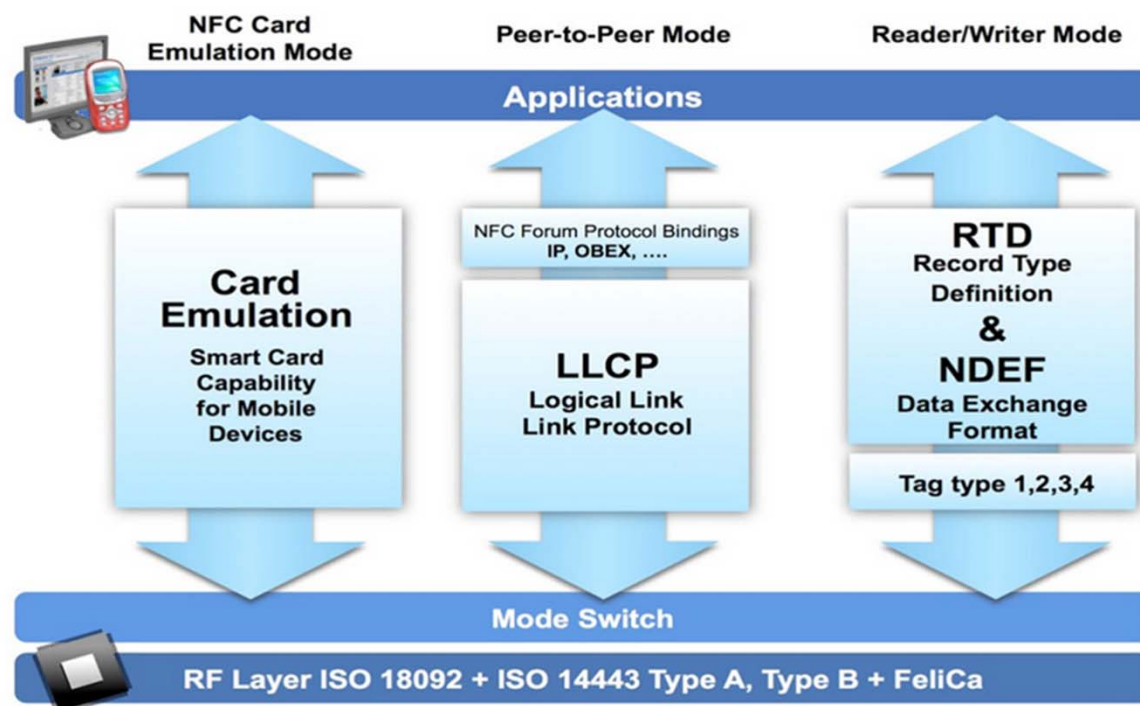
NFC Technology Brief

- Short range wireless technology – only a few cms
- Based on existing (legacy) contactless cards standards
- Data-Rates: 106-848Kbps (+ 1.65-26.48Kbps in legacy)
- Frequency-Band: 13.56MHz (ISM Band)



NFC and Interoperability

- NFC Forum specs are based on existing and recognized ISO/JIS standards, therefore, in many ways they can be considered as next step in the evolution of the HF RFID technology.
- Testing and certification is also evolving, with the Wave 1 compliance program is available now and tests for lower level digital protocols.
- As many released devices are not tested, the S2 MCU NFC group at TI is testing against released devices and starting the Wave 1 compliance testing as well.

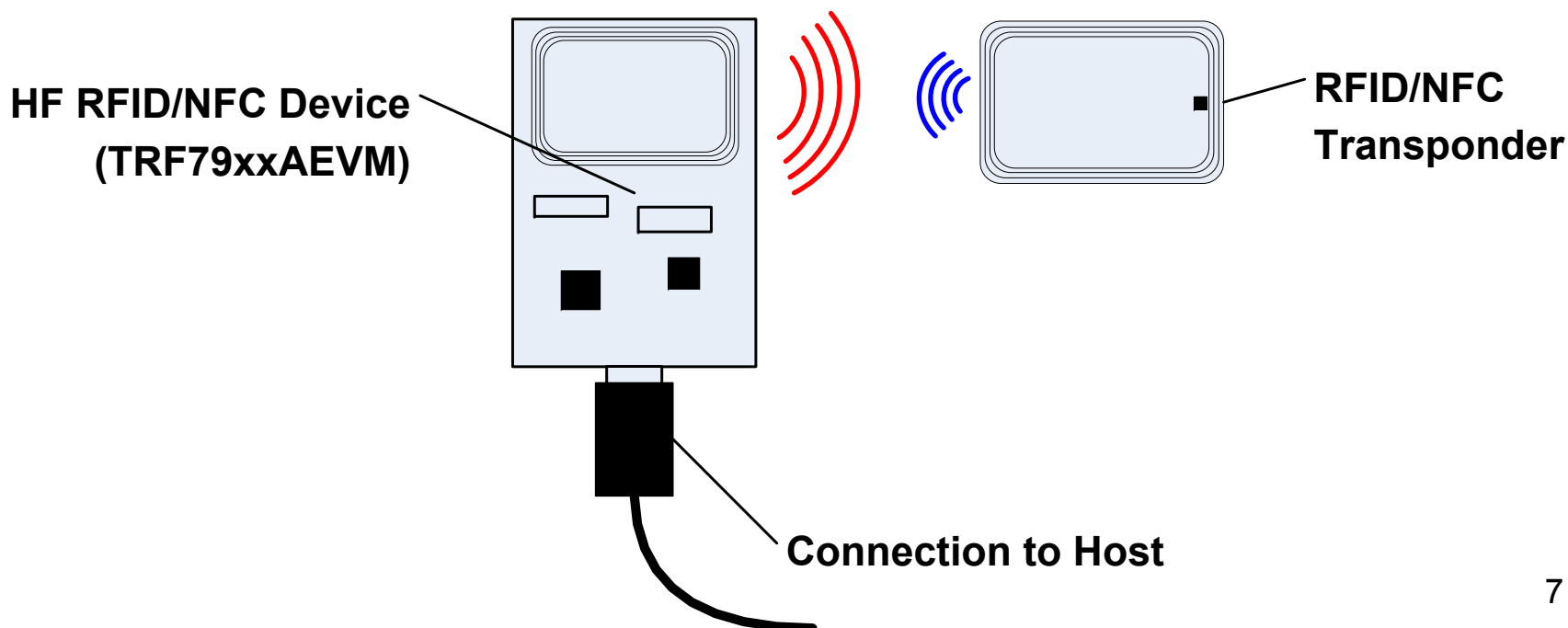


HF RFID/NFC Systems and Use Cases

- **Systems (Technical Components)**
 - RFID/NFC Systems
 - NFC Systems
- **Air Interface (Overview)**
- **Digital Protocols (Overview)**
- **Traditional and Emerging/Evolving Use Cases**

Passive HF RFID/NFC System Illustration

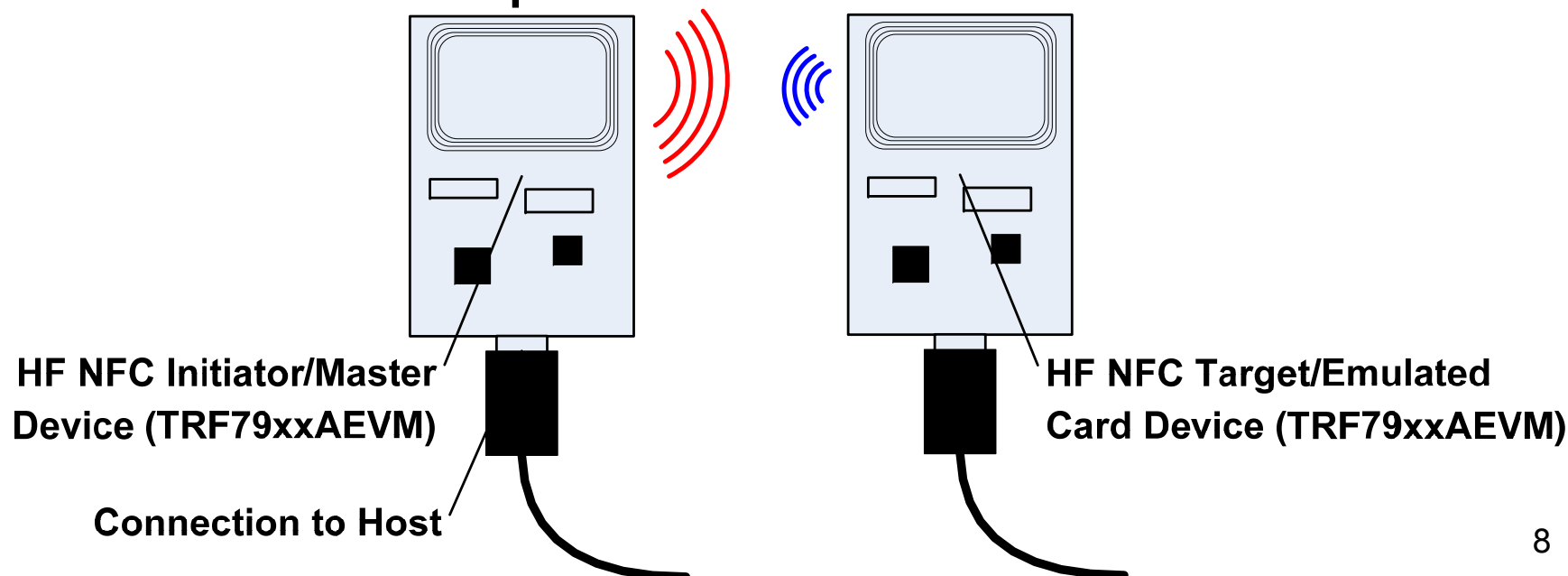
- **HF RFID/NFC Device – Initiates Communication via Downlink (Modulates Carrier according to Protocol Command)**
- **RFID/NFC Transponder (static tag) – load modulates its response back to the command**
- **This configuration is classic RFID use case.**



HF NFC

System Illustration

- **HF NFC Device (Master) – Initiates Communication via Downlink (Modulates Carrier according to Protocol Command)**
- **NFC Target or Emulated Card – modulates a response back to the command**
- **This configuration can be used for Peer to Peer or Card Emulation mode operations**



Air Interface Overview

- The RFID/NFC systems all use 13.56MHz carrier frequency.
- This is a regulated frequency worldwide ($\pm 7\text{kHz}$) and for our discussion of the TRF79xxA IC and associated low power systems, the output power of the systems is well below any limits imposed by regulatory agencies.
- We refer to the communication coming from the Initiator/Master as Downlink
- We refer to the communication from the tag/emulated card/target/slave as the Uplink

Air Interface

(as they relate to the Protocols)

- We must talk a little bit about the ISO protocols as they are what govern the communication fundamentally.
- The three main protocols used for RFID are: ISO14443A, ISO14443B and ISO15693
- NFC Protocols also use ISO14443A and B, but add one called NFC-F which is based on FeliCa (developed by Sony).

Protocol Type A, Type B and ISO15693 (Type V) Comparison

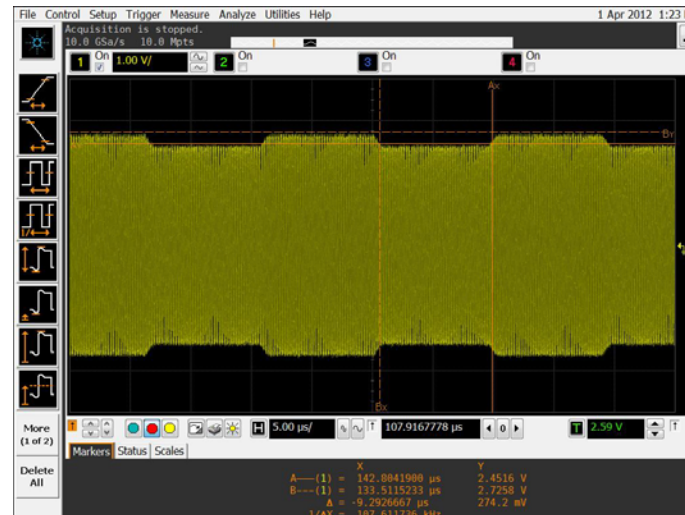
Technical Aspect	ISO14443A	ISO14443B	ISO15693	General Comments (For more specific feedback, pls request further info)
Origins	~1990	~1995	~2001	Type B was derived at a much later date than Type A, so has a number of advantages.
Data Rate	106 Kbs	106 up to 847 Kbs	1.65/26.4 kbs	Type B is adaptable to application speed requirements. 14443-3 supports negotiation of higher data-rates with Type B.
Anti-Collision	Medium Binary-search-tree with inefficiencies	Excellent Slotted-ALOHA with dynamic slot adaptation by reader	Excellent Slotted deterministic concept	Type B Slotted ALOHA is the more efficient and sophisticated anti-collision mechanism compared to binary tree search.
Multi-Applications	Yes - Medium	Yes - Fast	Yes - Slow	No clock recovery required with Type B for multi-applications.
Modulation Depth	100% (NO data processing DURING off pulses)	10% (Data processing DURING off pulses)	100% and 10%	100% modulation may offer greater noise immunity for long read-range applications >0.5-1m , but no difference for small read-range applications <.1m.
Air-Interface Complexity	Low (only 100%)	Low (only 10%)	Medium (10% and 100%)	Limited differences in air-interface complexity when using fixed depths of modulation.

What does the Air Interface Downlink Look like?

- 100% ASK/OOK Example
(for ISO14443A/ISO15693)



- 10% ASK Example
(for ISO14443B/FeliCa)



ISO14443A Downlink Example

ISO14443A Standard

Important Timings

- $128/f_c = 9.435\mu\text{Sec} = t_b$ (106kbps data rate)
- $64/f_c = 4.719\mu\text{Sec} = t_x$ time
- $32/f_c = 2.359\mu\text{Sec} = t_1$ time

Figure 10 together with the timing parameters in Table 7 illustrate sequences X, Y and Z.

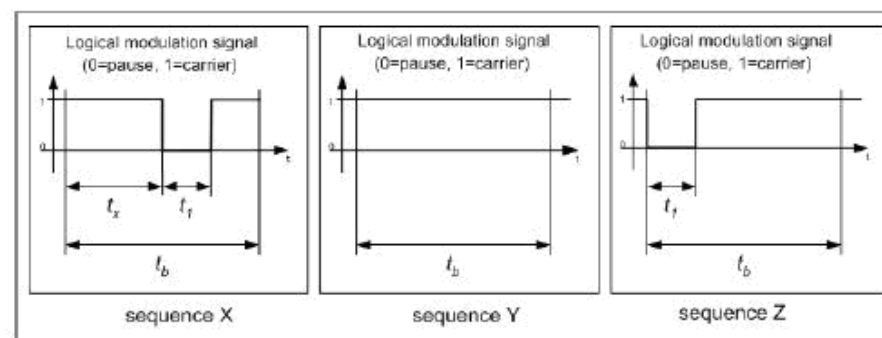


Figure 10 — Sequences for Type A communication PCD to PICC

Table 7 — Parameters for sequences

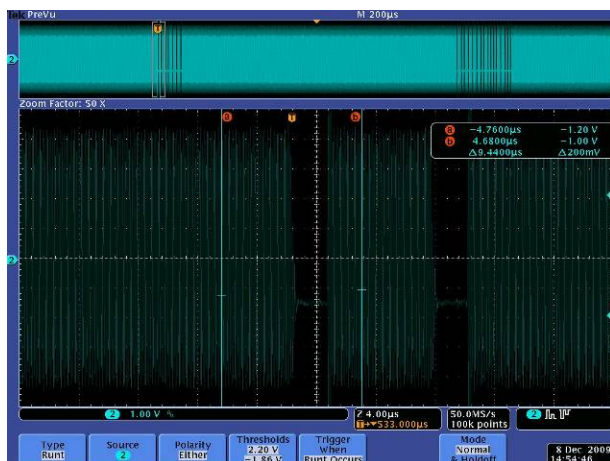
Parameter	Bit rate			
	$f_c/128$	$f_c/64$	$f_c/32$	$f_c/16$
t_b	$128/f_c$	$64/f_c$	$32/f_c$	$16/f_c$
t_x	$64/f_c$	$32/f_c$	$16/f_c$	$8/f_c$
t_1	see t_1 of Table 3	see t_1 of Table 5		

The above sequences shall be used to code the following information:

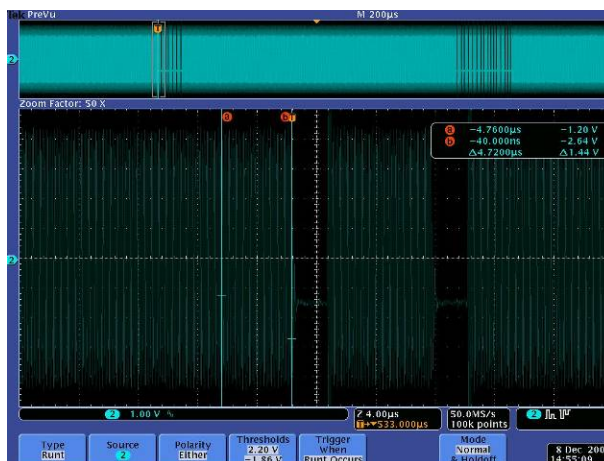
- logic "1": sequence X,
- logic "0": sequence Y with the following two exceptions:
 - i) If there are two or more contiguous "0"s, sequence Z shall be used from the second "0" on,
 - ii) If the first bit after a "start of frame" is "0", sequence Z shall be used to represent this and any "0"s which follow directly thereafter,
- start of communication: sequence Z,
- end of communication: logic "0" followed by sequence Y,
- no information: at least two sequences Y.

ISO14443A Analog Screen Captures

- These captures illustrate sequence X, as taken from the TRF7960EVM



$$t_b = 9.44\mu\text{Sec}$$



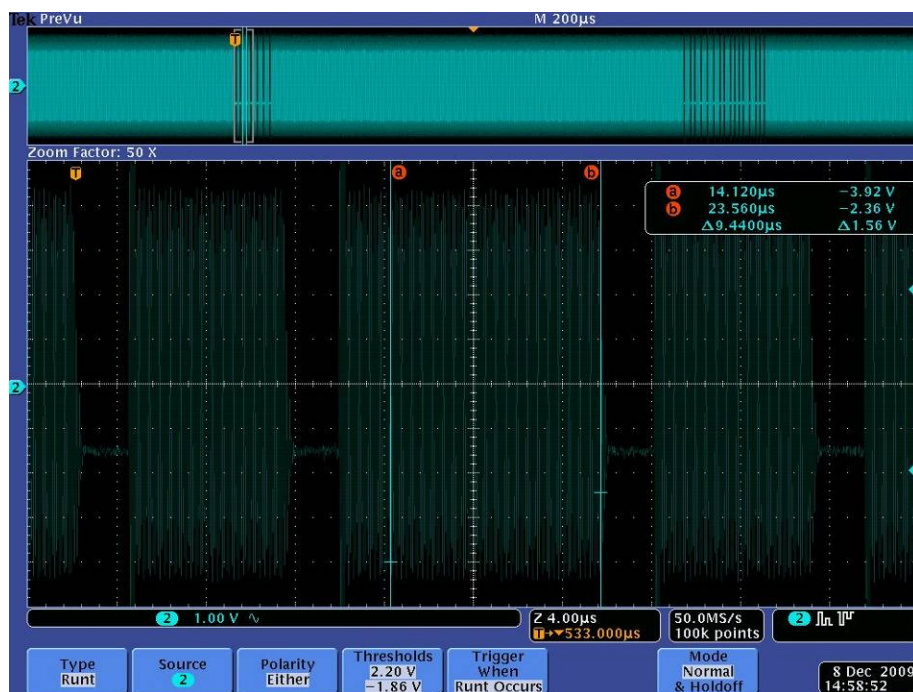
$$t_x = 4.72\mu\text{Sec}$$



$$t_1 = 2.48\mu\text{Sec}$$

ISO14443A Analog Screen Captures

- These captures illustrate Sequences Y and Z, as taken from the TRF7960EVM

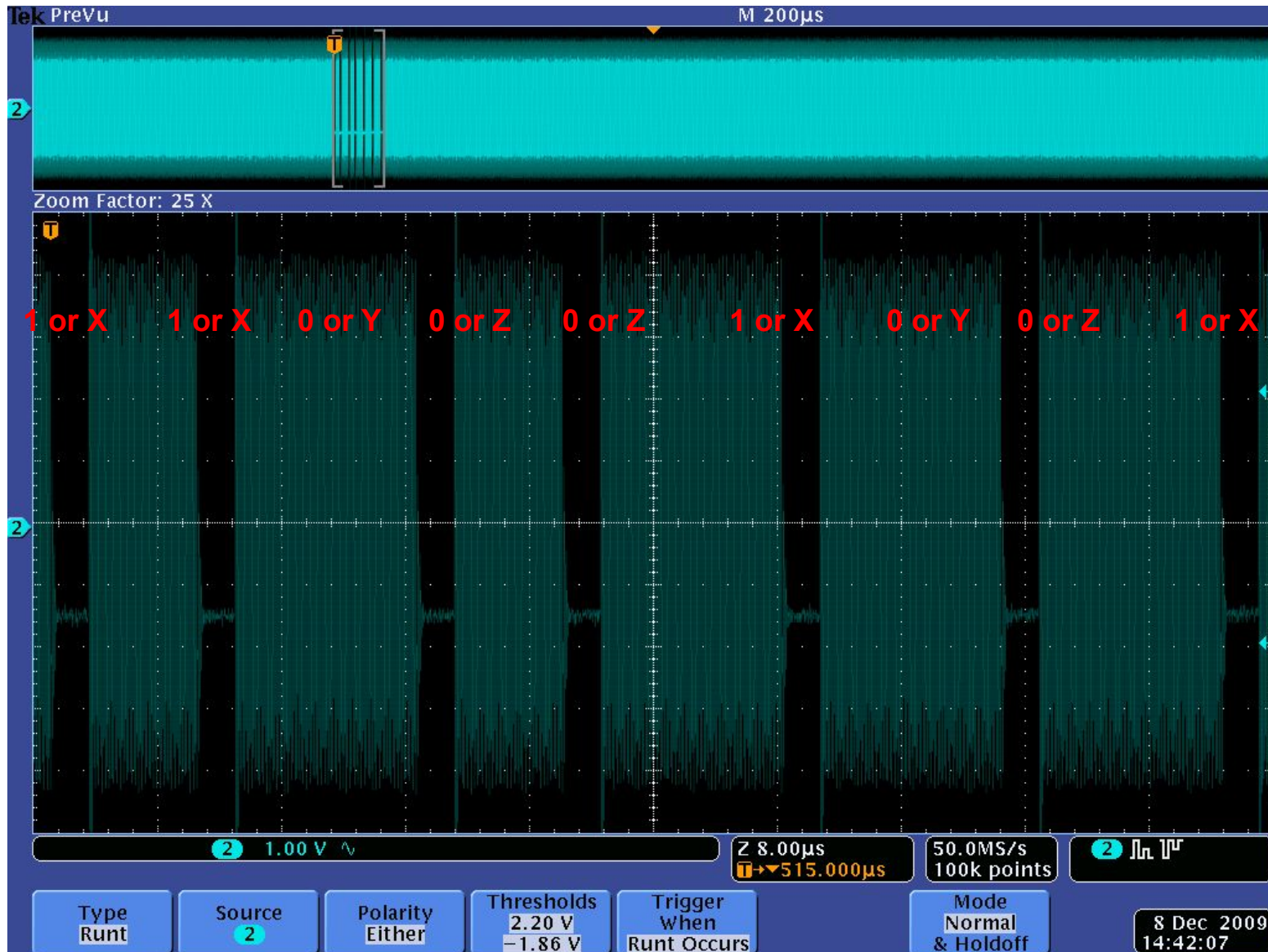


Sequence Y = Carrier for 9.44uSec



Sequence Z = Pause for 2uSec-3uSec,
Carrier for Remainder of 9.44uSec

ISO14443A Analog Screen Capture Decoded

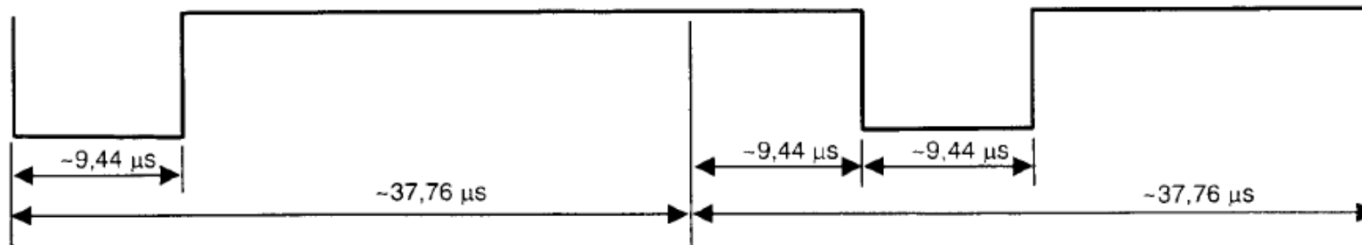


ISO15693 Downlink Example

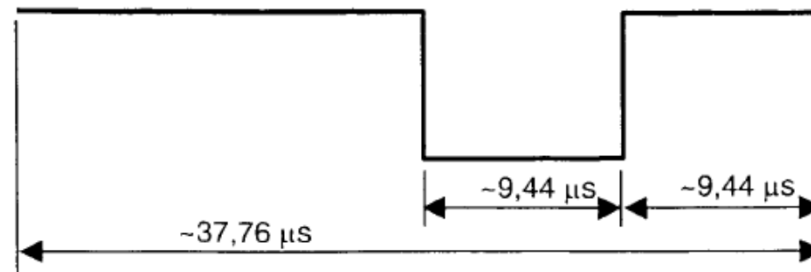
ISO15693 Standard

Important Timings

- Start of Frame (SOF)



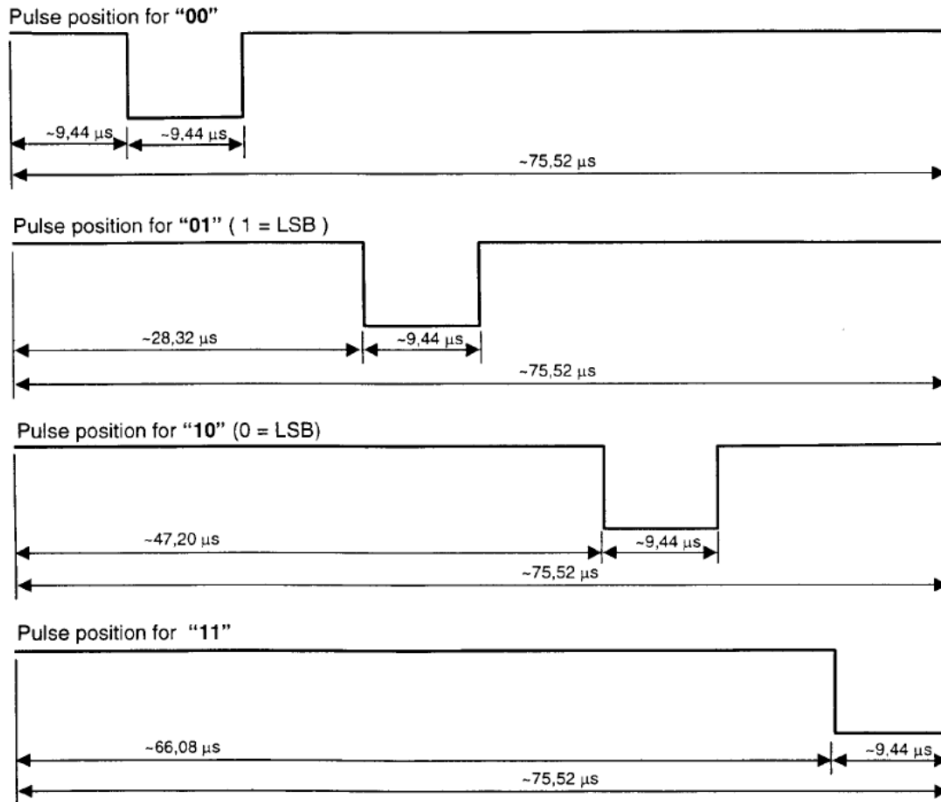
- End of Frame (EOF)



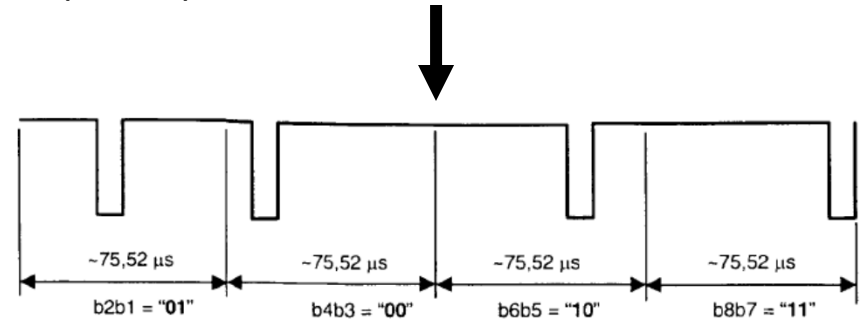
ISO15693 Standard

Important Timings (cont.)

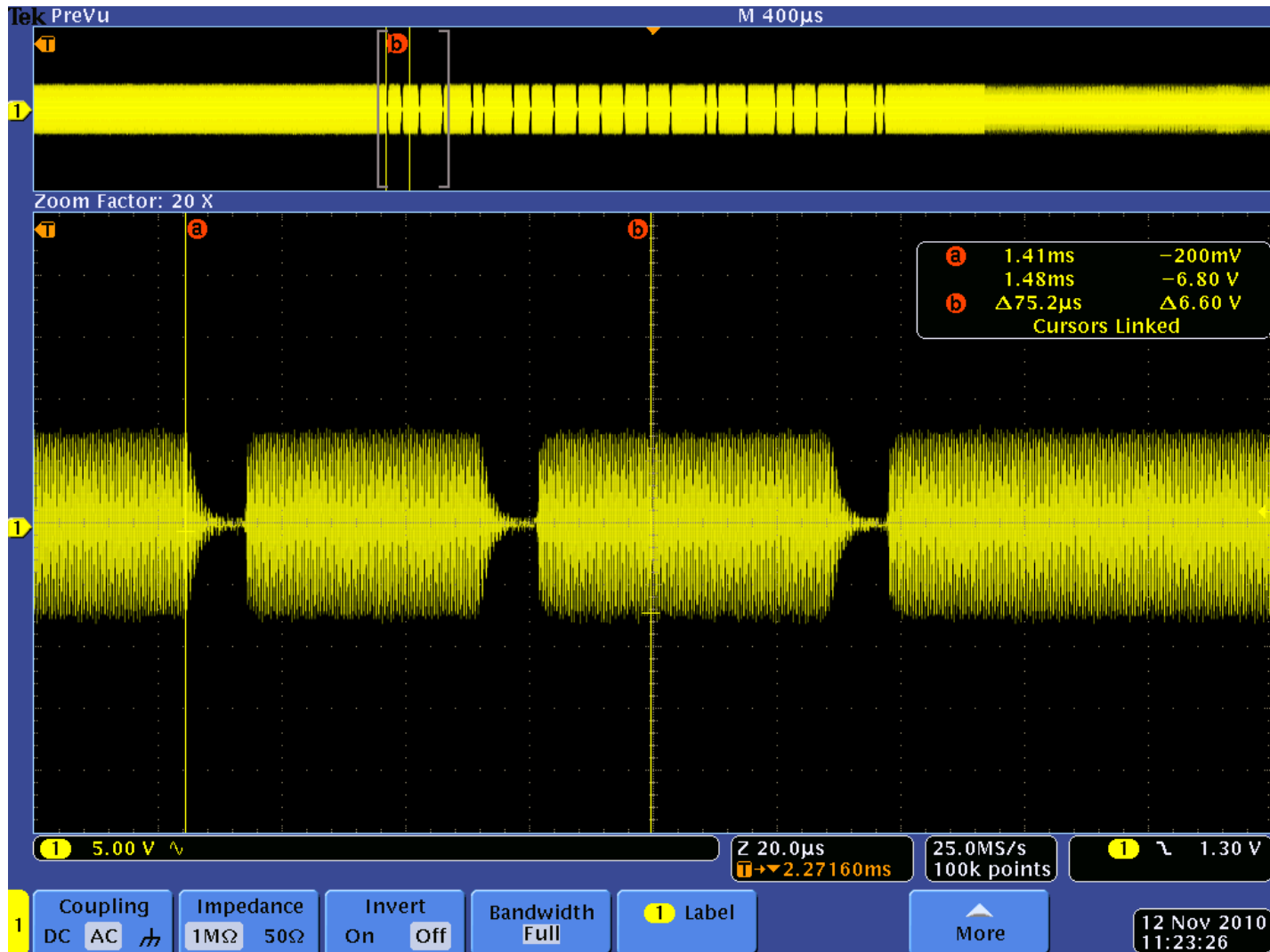
- Symbols 00, 01, 10, 11
 - Pulse Position Modulation Technique is used here, where the position determines two bits at a time.



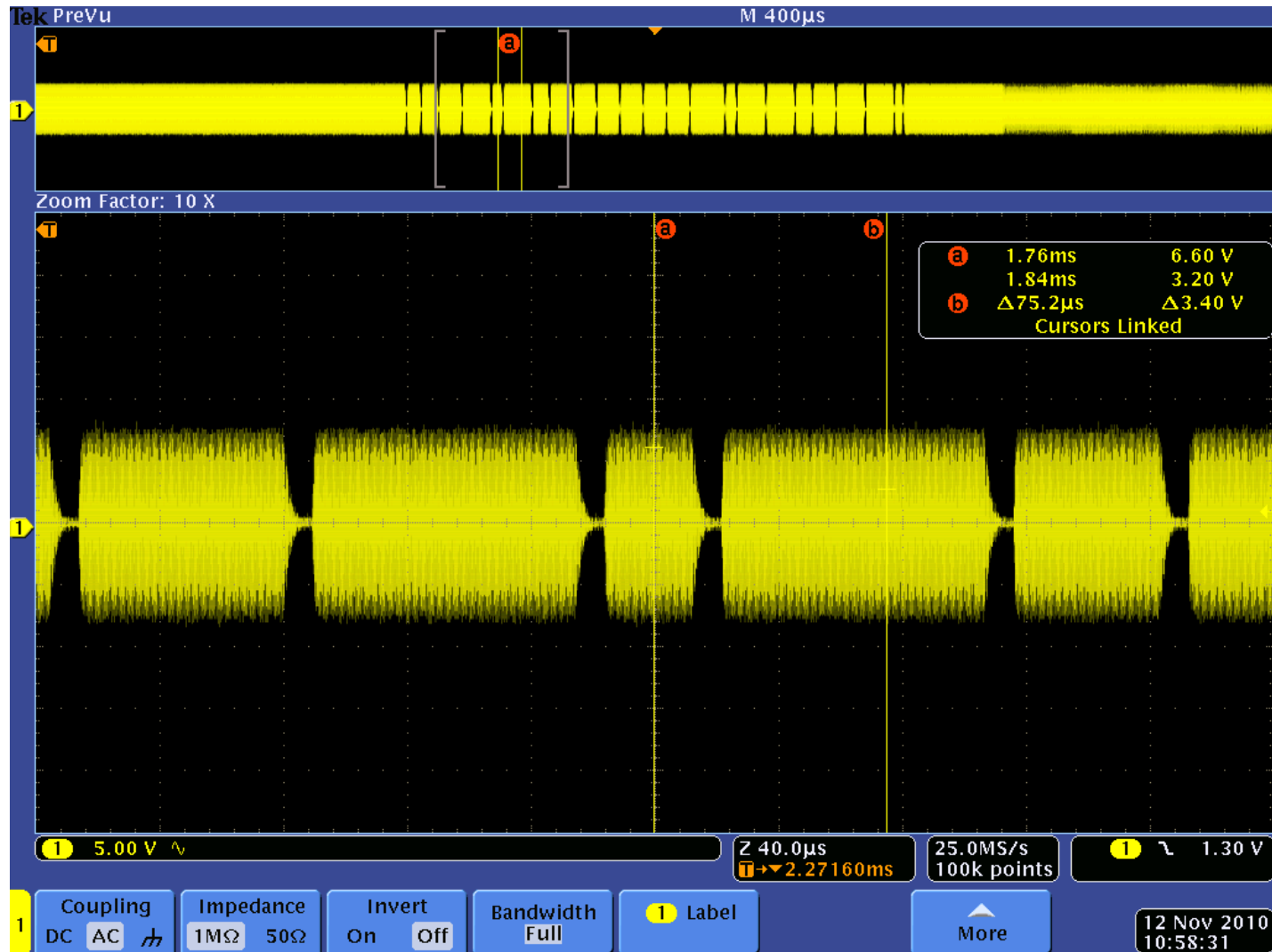
This is showing one complete byte (0xE1) for transmission



ISO15693 Start of Frame (SOF)



ISO15693 Symbol 00



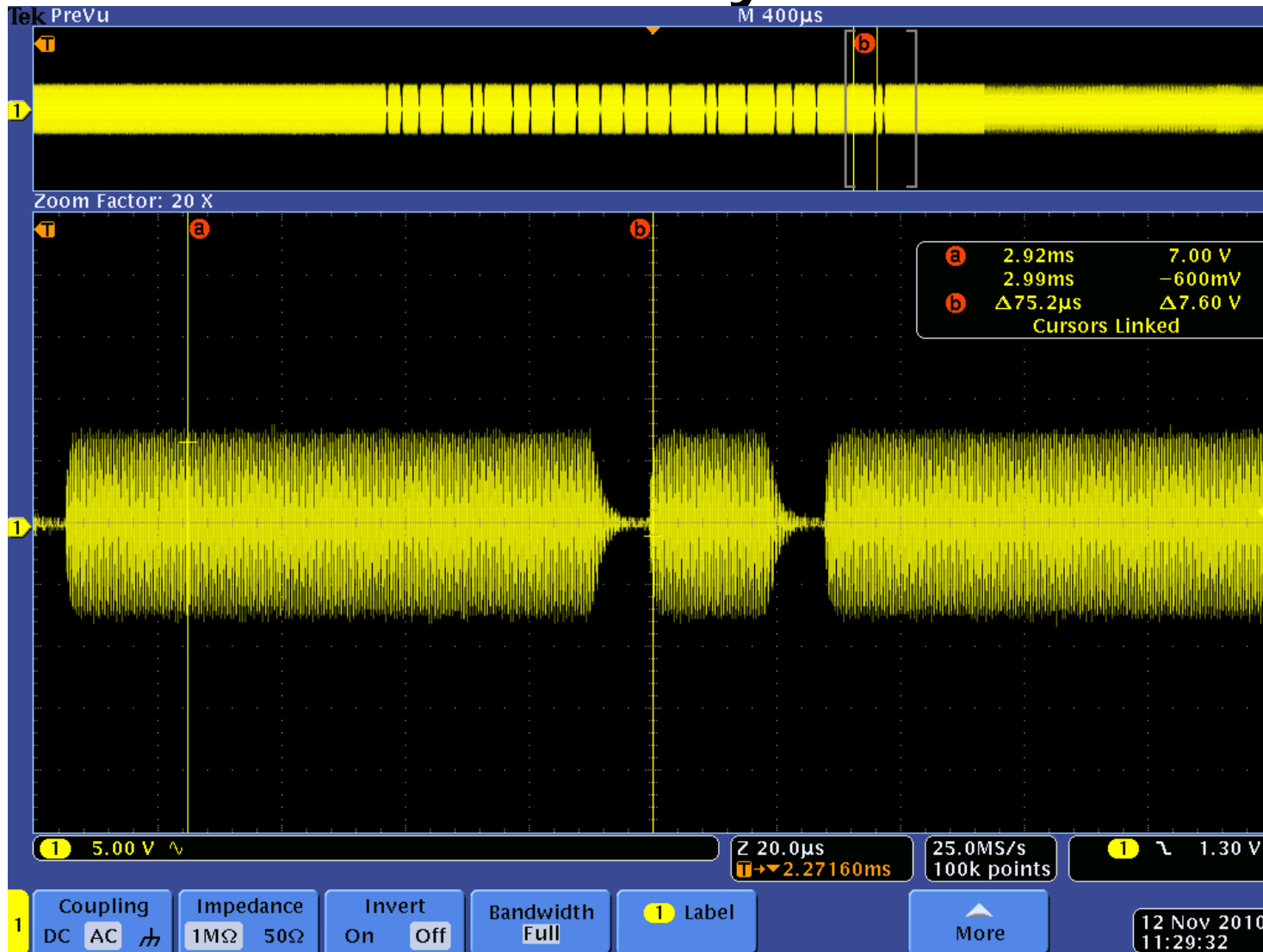
ISO15693 Symbol 01



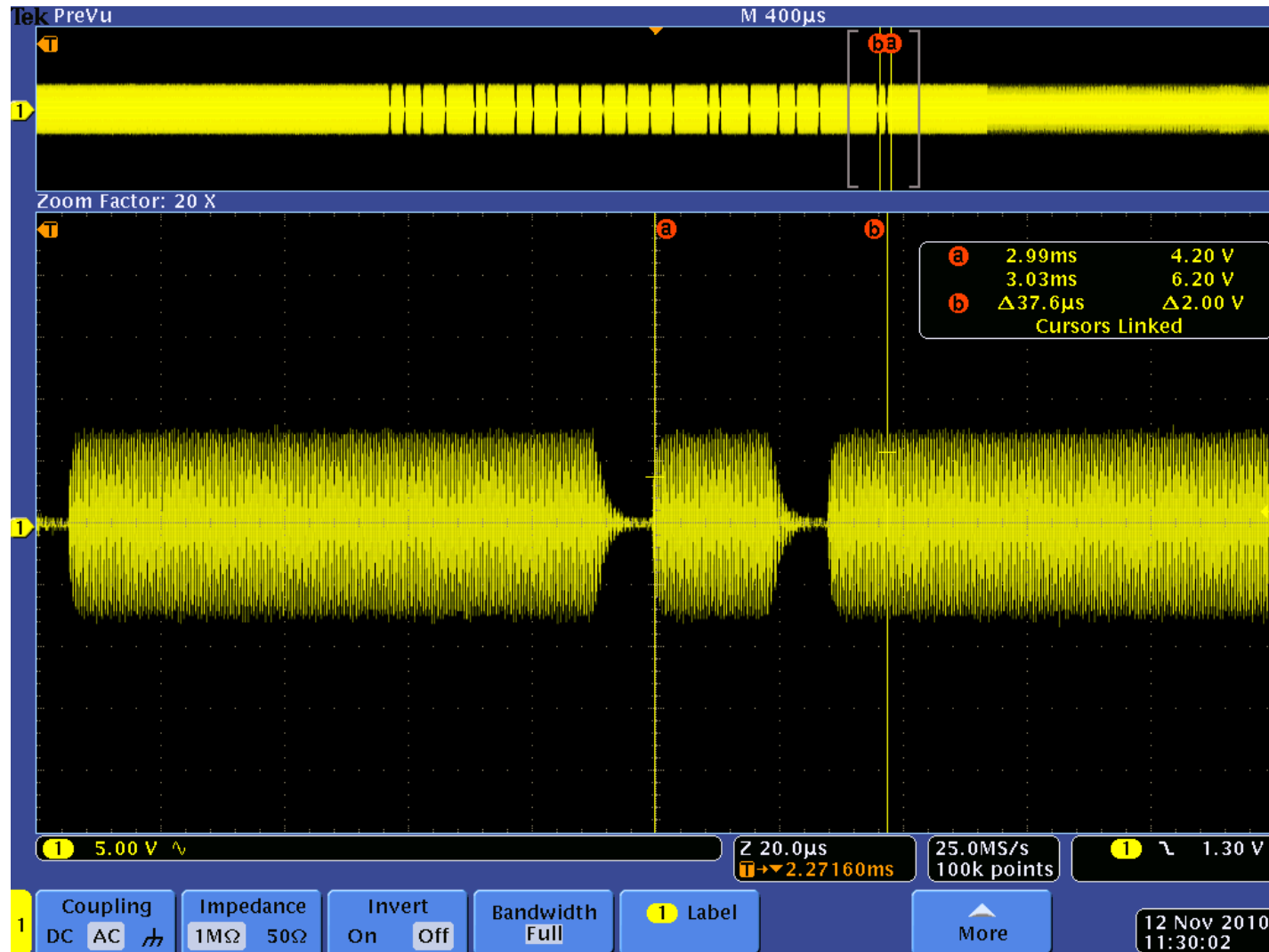
ISO15693 Symbol 10



ISO15693 Symbol 11



ISO15693 End of Frame (EOF)



Quick Analog Conclusion

- The preceding slides were not to overwhelm you - just to show that there is an air interface protocol which is being controlled by the digital domain.
- For default RFID/NFC operations, the TRF79xx devices handle all of the analog, but still need a robust controller firmware driving it.
- Conclusion – MCU firmware is still a crucial part of any successful implementation of this highly integrated RFID/NFC transceiver IC.

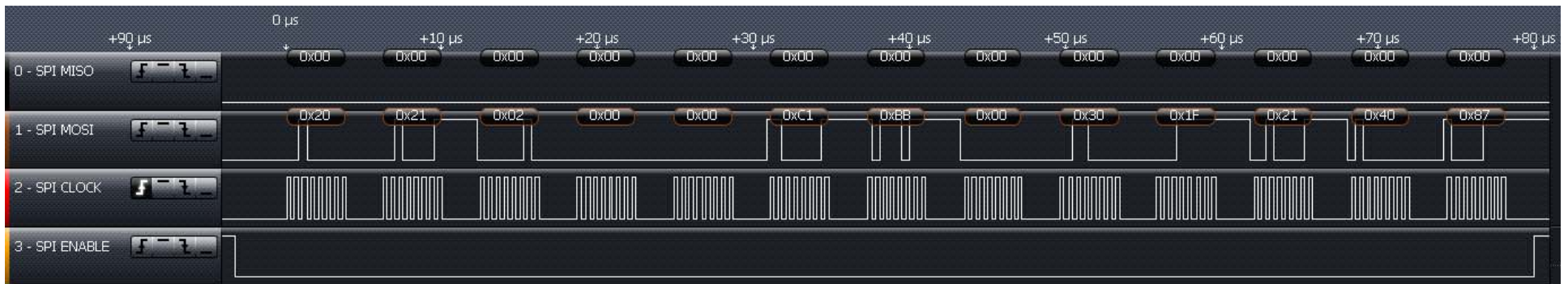
ISO15693 Digital Protocol Example

Digital Protocol Domain

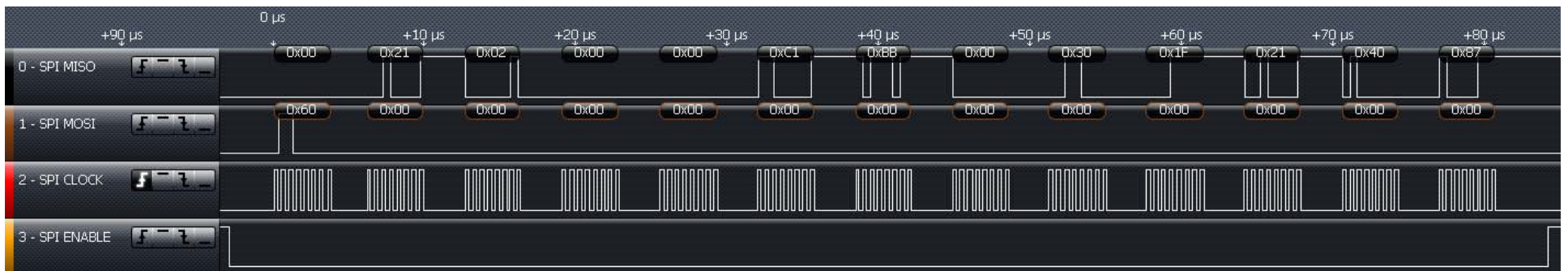
- Within the timeframe we have here today, I will show some example here of the MCU and the TRF79xx device performing some basic operations.
 - Configuration of RFID/NFC IC Registers
 - Read Back of Registers (Verifying the Register Write)
 - Issuance of a Command
 - Interrupt Handling
 - Retrieval of a Response
- These slides are to illustrate some SPI communication between the RFID/NFC IC and the MCU (in this case an MSP430)

Write and Verify Registers

- Continuous write for configuring registers 0x00 : 0x0B

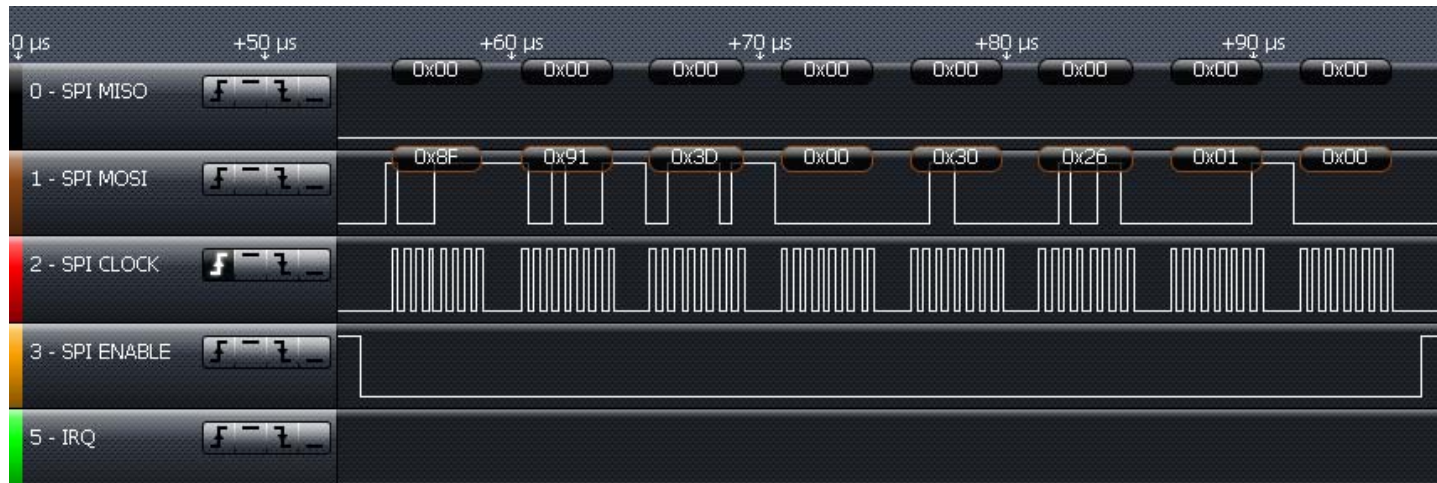


- Continuous read for configuring registers 0x00 : 0x0B

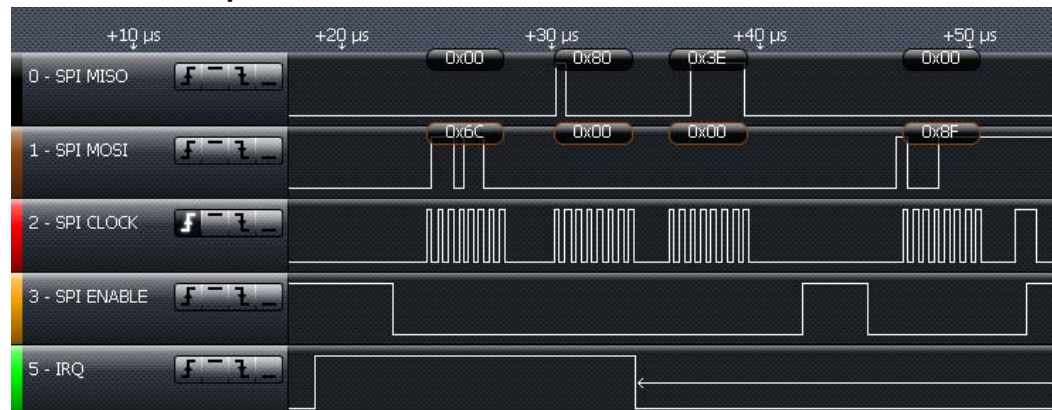


Issuance of a Command (Inventory Example)

- Inventory Command (Single Slot)

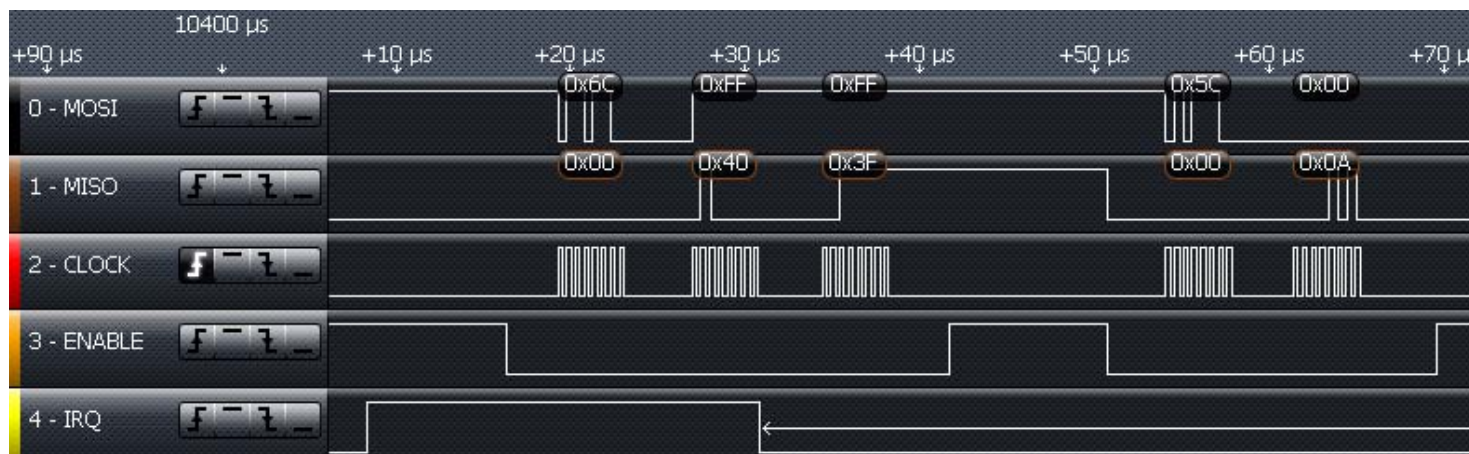


- End of Transmit Interrupt

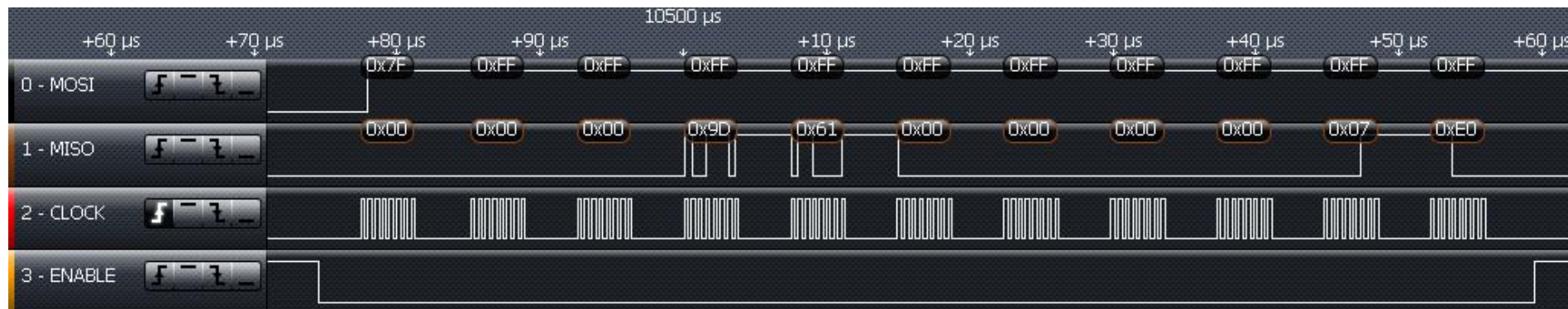


Issuance of a Command (Inventory Example, cont.)

- End of RX IRQ and FIFO Status Read (10 bytes in FIFO, expected)

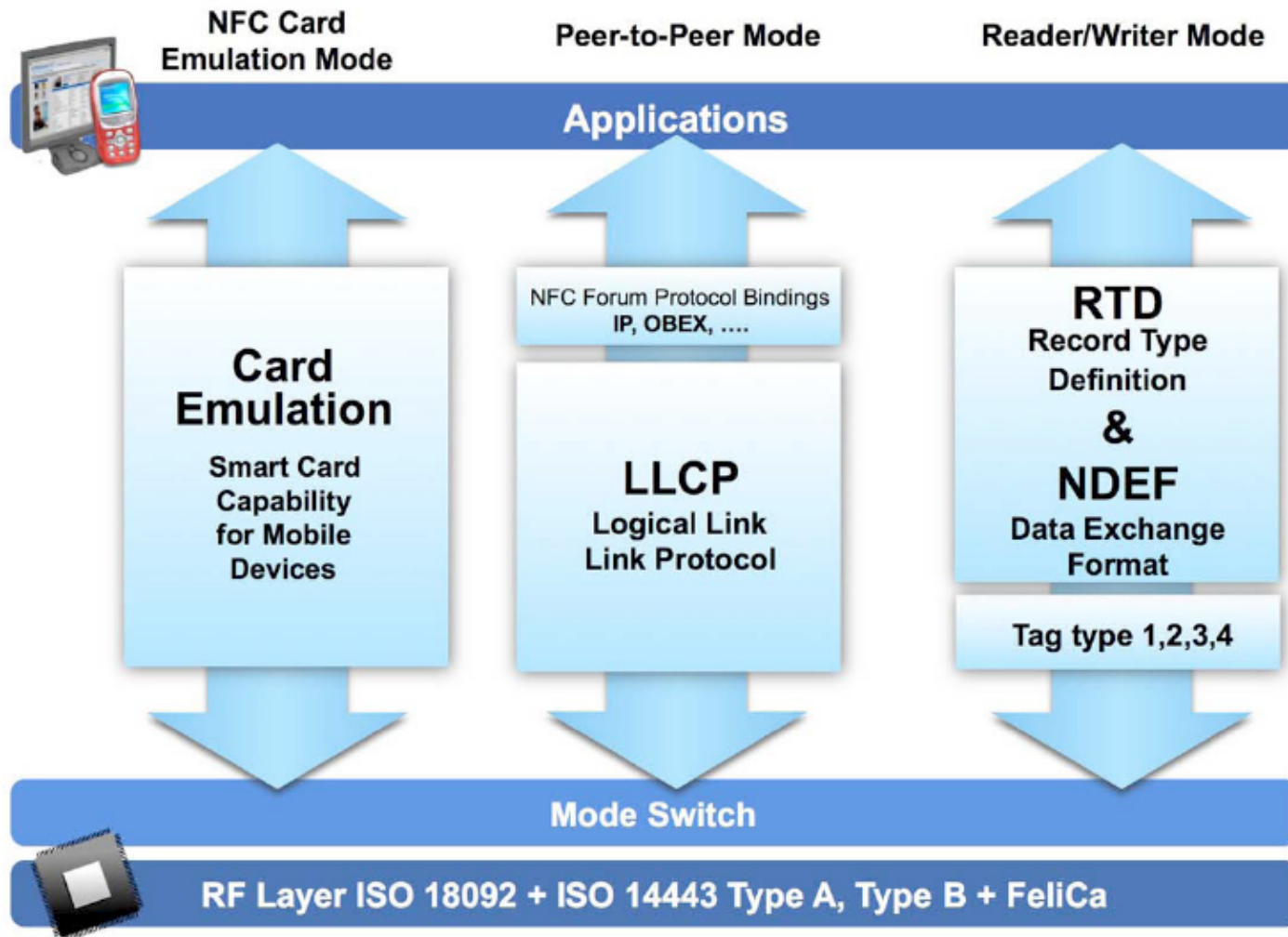


- Read FIFO for the tag UID (= 0xE00700000000619D, DSFID = 0x00, Flags = 0x00)





NFC Technology Architecture



NFC Terminology

Initiator (master)

- Generator of the RF field and is the starter of the NFCIP-1 communication

Target (Slave)

- Responds to Initiator command either using load modulation scheme (passive mode) or using modulation of self generated RF field (active mode)

Active communication mode

- Both devices Target and Initiator have power supplies
- Both devices (Initiator and the Target) generate their own RF field for the communication
- This is the mode preferred for Peer to Peer communication

Passive communication mode

- Both devices Target and Initiator have power supplies
- Only the initiator generates the RF field for the communication
- The Target responds to an Initiator command by **applying a load modulation** on the RF field
- This is the mode is used for:
 - Peer to Peer communication
 - Reader/Writer
 - Tag Emulation

NFC Terminology (cont.)

Peer to Peer mode

- Peer to Peer mode provides a communication between two devices where both devices are able to initiate communications when required.

Card Emulation mode

- In Card Emulation mode a NFC device is able to behave like a Contactless Smartcard. A NFC device may have the ability to emulate more than one card.

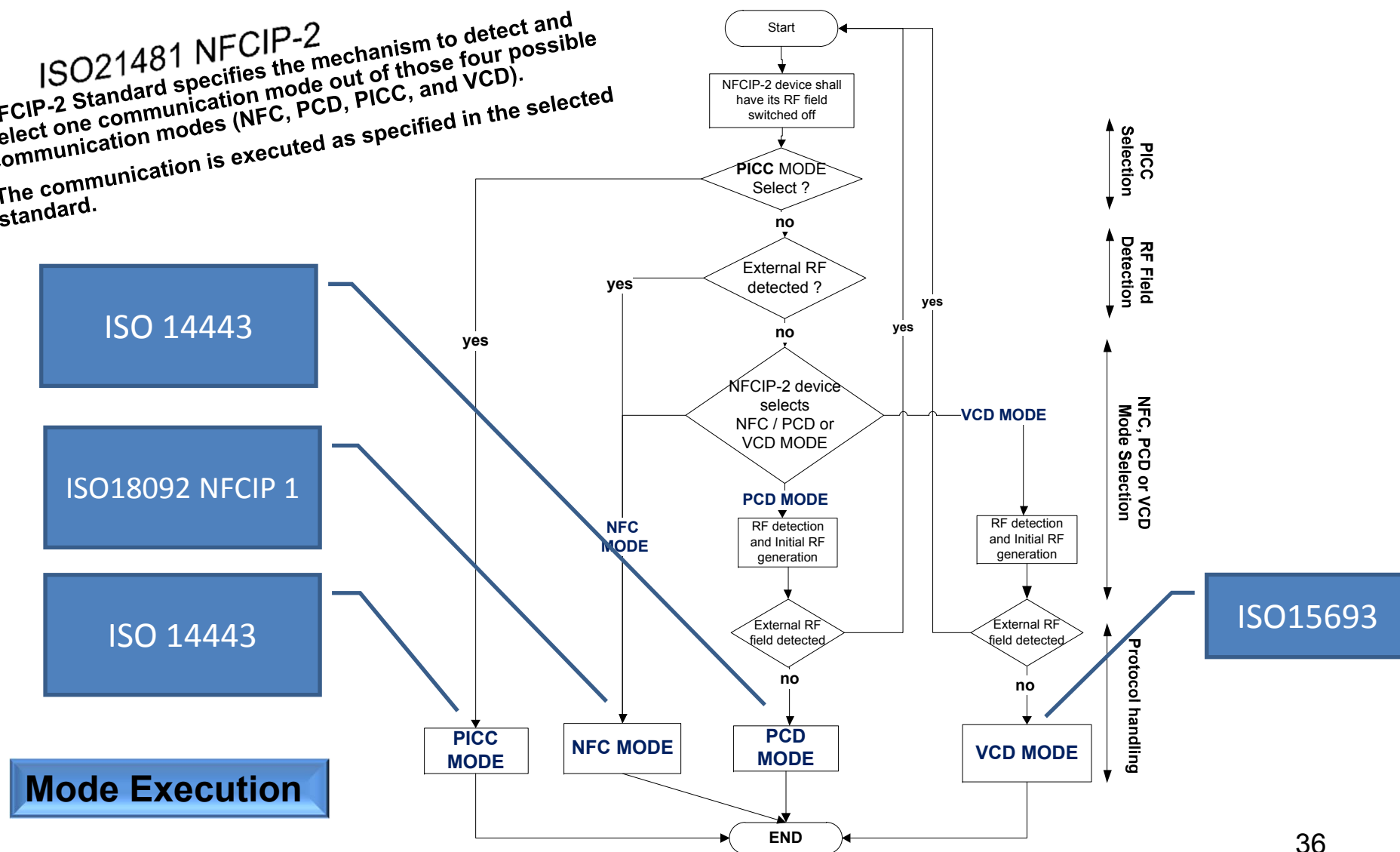
Reader/Writer mode

- A Reader/Writer NFC device has the ability to read data from, and write data to RFID and Contactless Smartcards



NFC Interoperability Flow

ISO21481 NFCIP-2
NFCIP-2 Standard specifies the mechanism to detect and select one communication mode out of those four possible communication modes (NFC, PCD, PICC, and VCD).
The communication is executed as specified in the selected standard.



BREAK

System Approach to Using TRF796x/6xA/70A

System Approach to Using TRF796x/6xA/70A

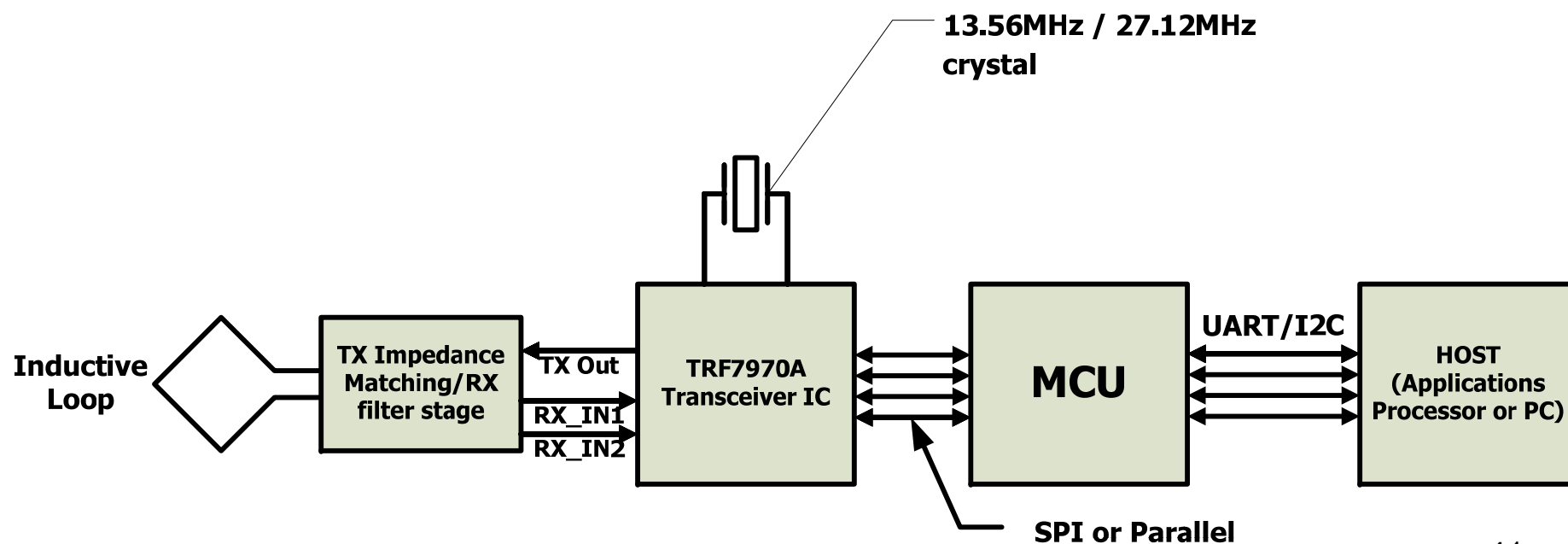
- TRF79xx Overview**
- Basic Electrical Connections/Circuit Examples**
- Impedance Matching RF TX/RX Circuit**
- RF Test Point Signals**
- Impedance Matching Antenna Circuit**
- Application Requirements driving MCU, TRF options**

Links to ti.com collateral for the TRF7970A and NFC

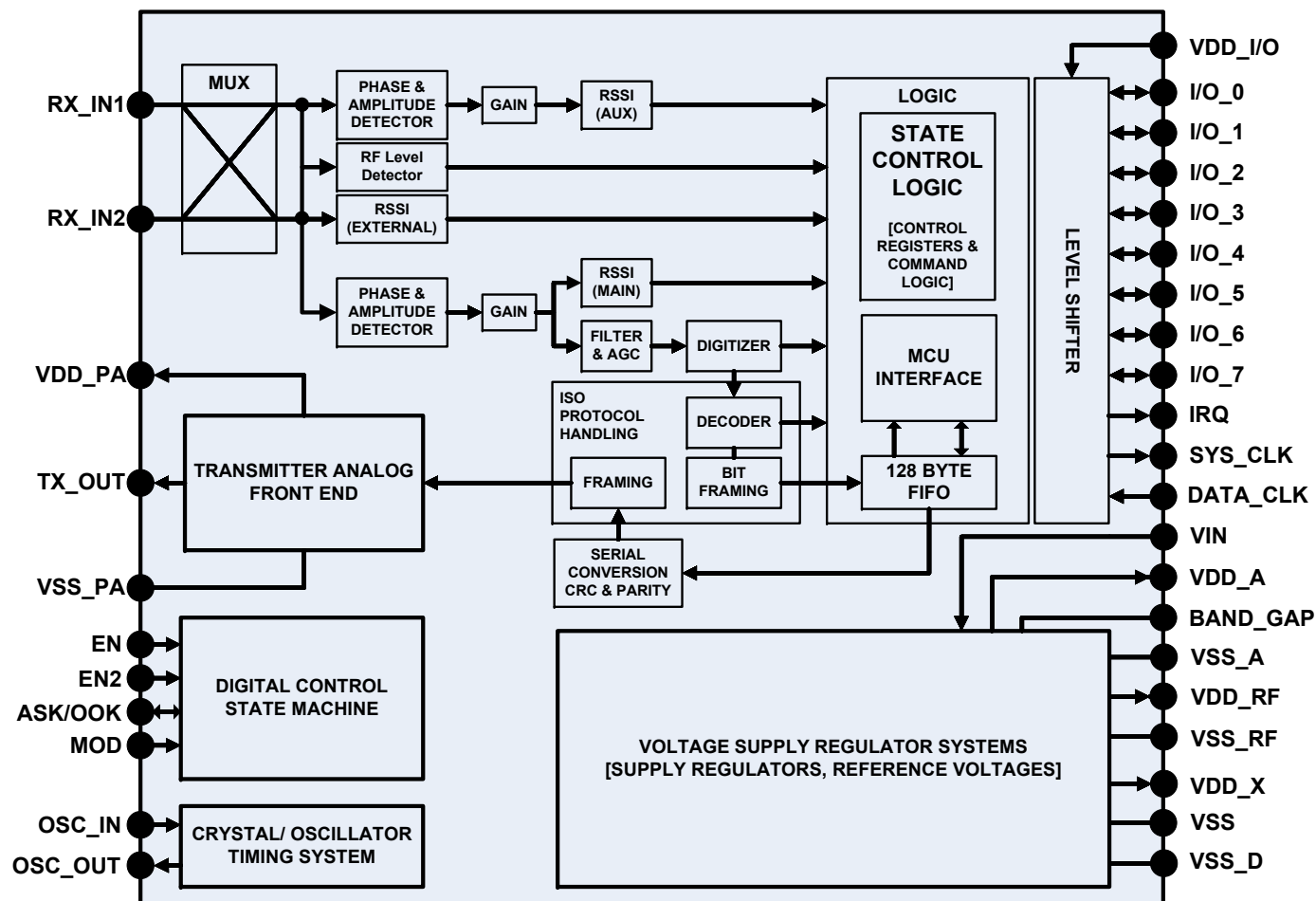
- NFC Landing Site
 - http://www.ti.com/llds/ti/microcontroller/near_field_communications/overview.page?DCMP=EmbeddedRF&HQS=nfc
 - Here we have application notes, source code and other collateral.
- TRF7970A Data Sheet
 - <http://www.ti.com/lit/ds/symalink/trf7970a.pdf>

TRF79xx + MCU based RFID/NFC device creation

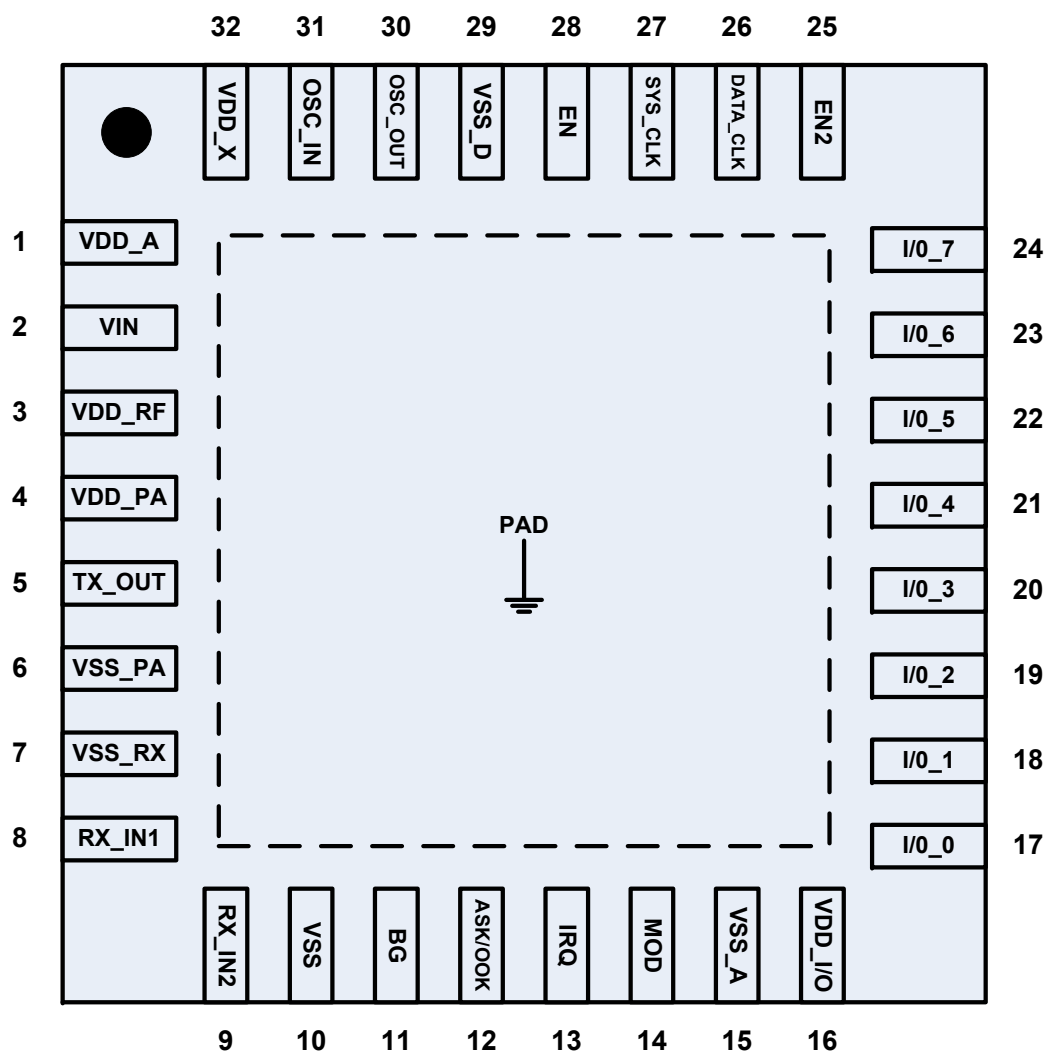
- Now we have covered some basic introduction to the RFID/NFC operations we can talk about the technical circuit creation side, then some firmware considerations.
- Below is simple block diagram for reference.



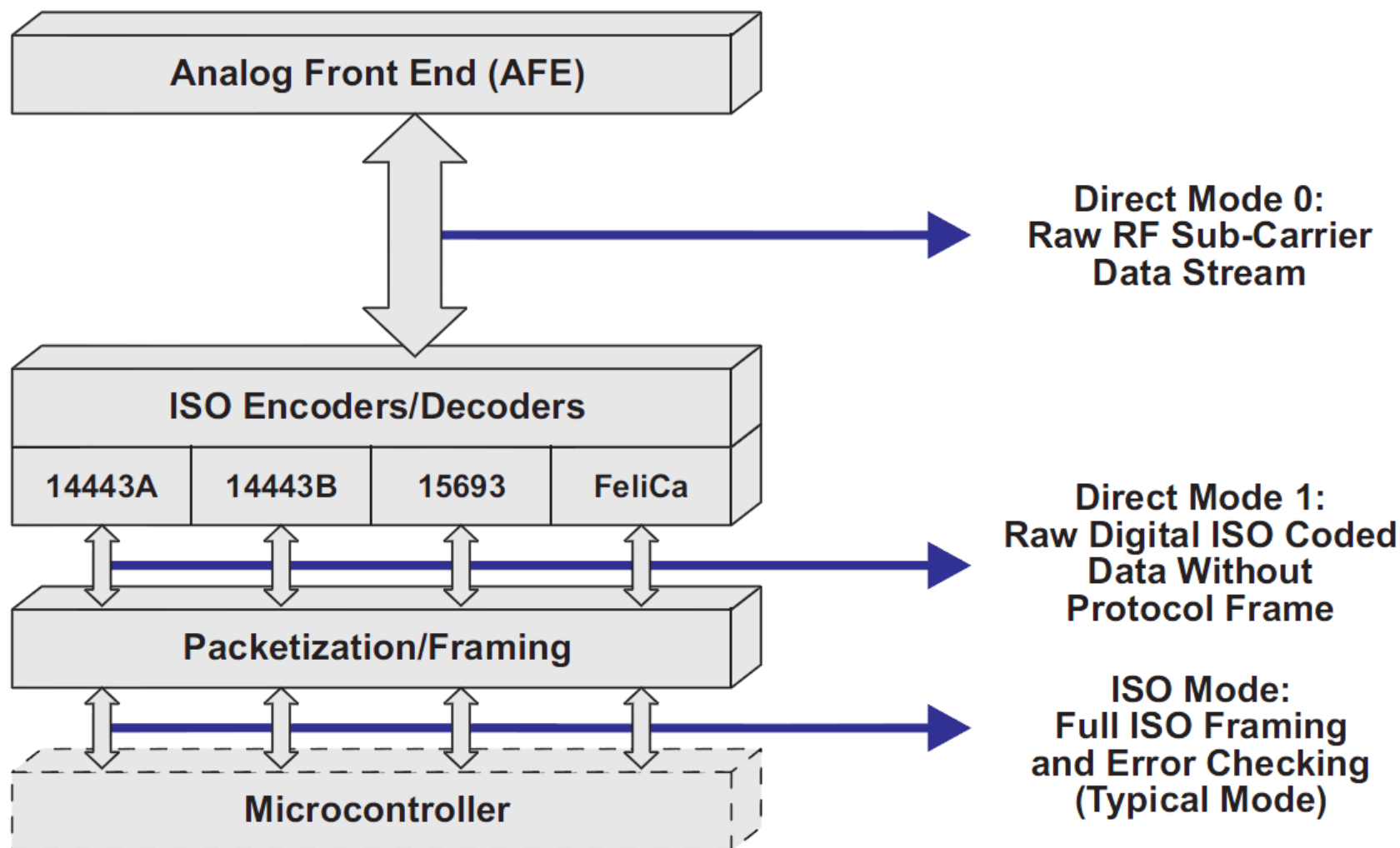
TRF7970A IC Block Diagram



TRF7970A IC Pinout (Top View)

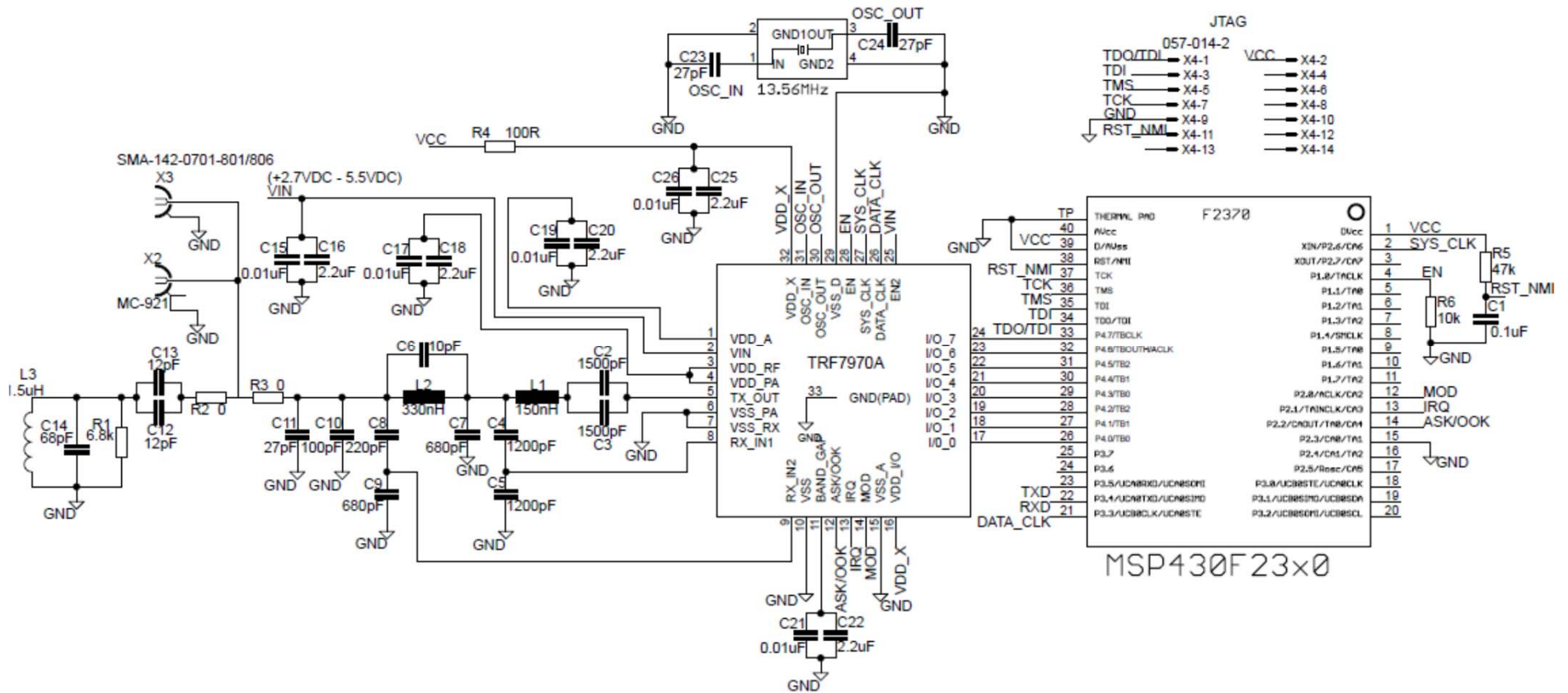


TRF7970A User-Configurable Modes





Circuit Diagram (Parallel)

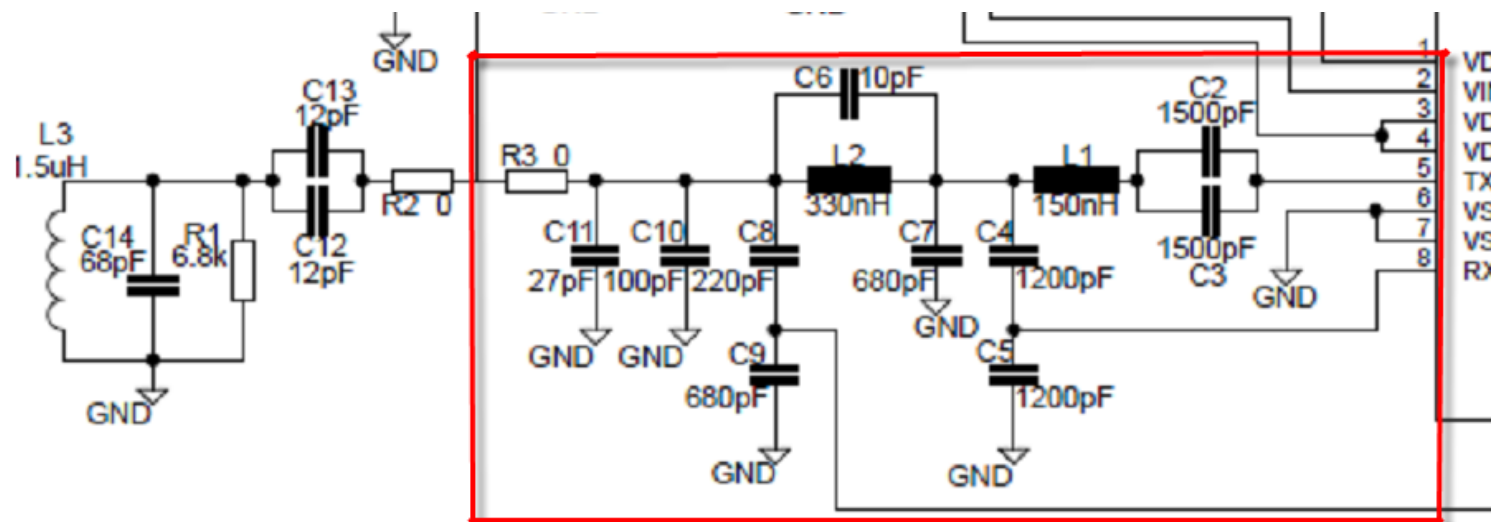


Impedance Matching Circuit from TRF79xx out to Antenna

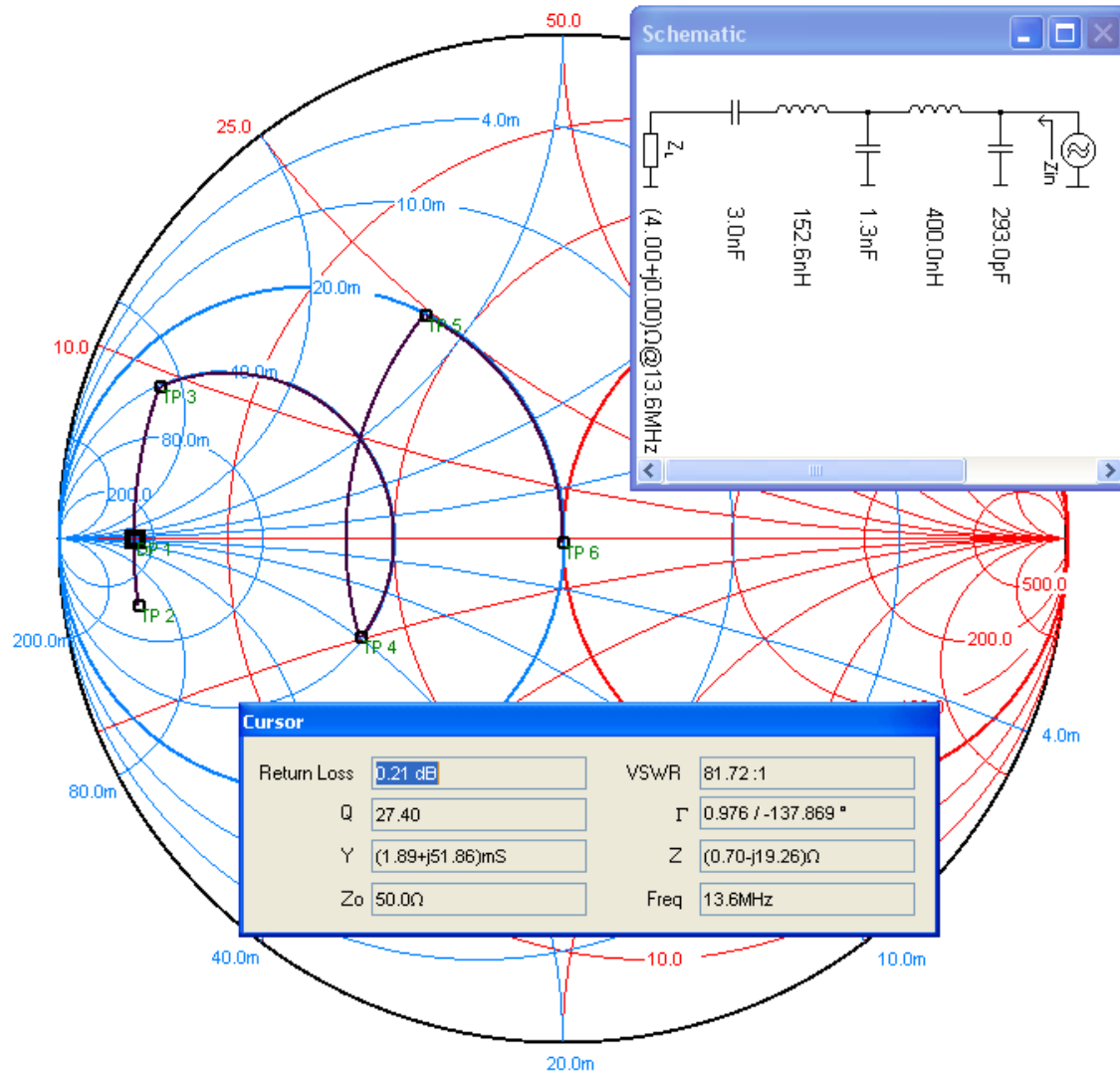
- The circuit diagrams previously show (SPI and Parallel) share the same RF section matching and this circuit is also common across the TRF79xx family of devices.
- The reference circuit is known good and customers should copy it – but for your complete understanding here we will explain the impedance match directly, then show the RF test point signals.

Impedance Matching Circuit from TRF79xx out to Antenna (cont.)

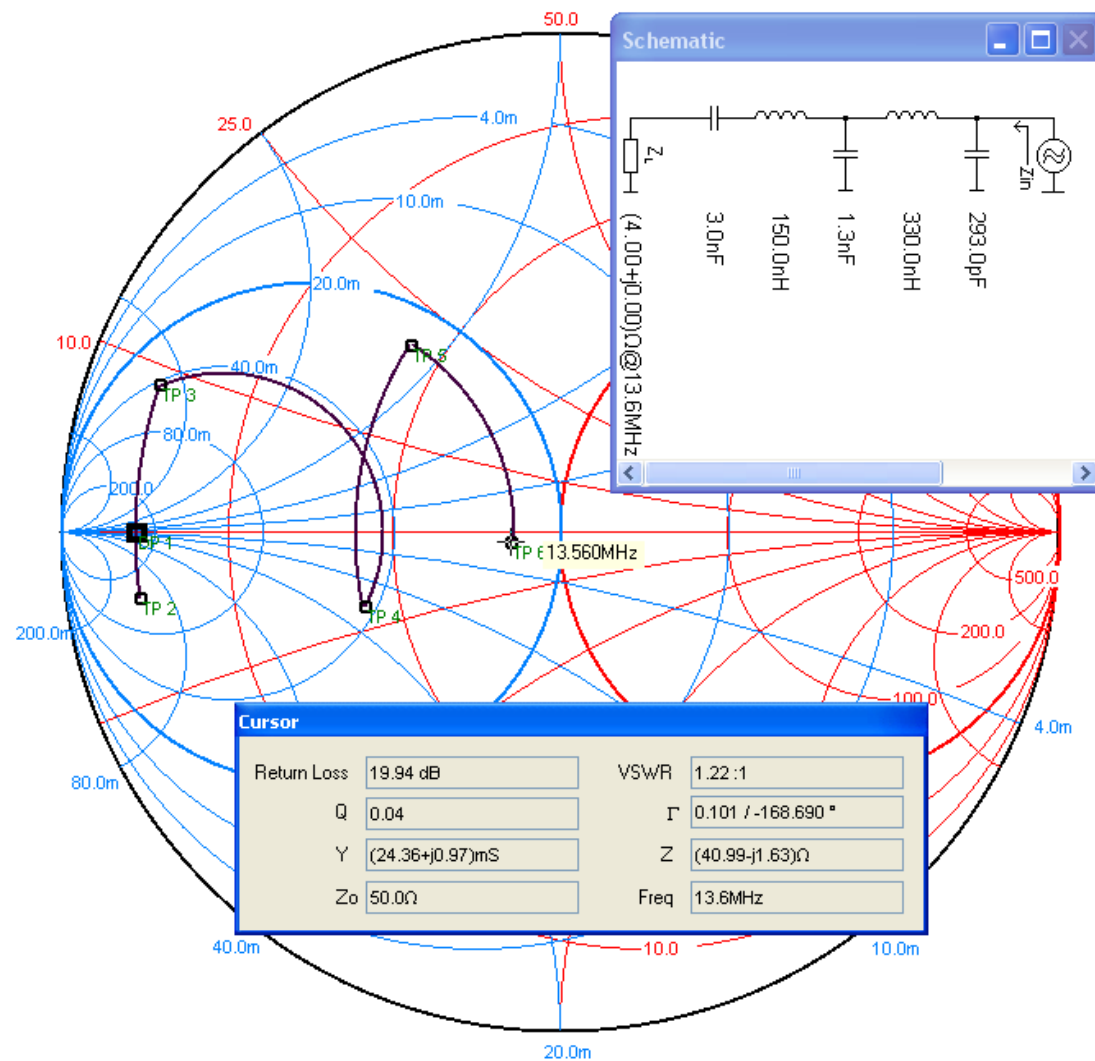
- The TRF79xx parts exhibit $\sim 4\ \Omega$ output impedance which must be impedance matched to $50\ \Omega$ in order to connect to matched $50\ \Omega$ antenna (for full power transfer)
- The easiest way to show this is to lump the elements of the circuit and express on a Smith Chart for verifying values, then moving to standard values available for low cost production worthy circuit.
- The section outlined in red is what we are discussing now.



Impedance Matching Circuit from TRF79xx out to Antenna (cont.)



Impedance Matching Circuit from TRF79xx out to Antenna (cont.)



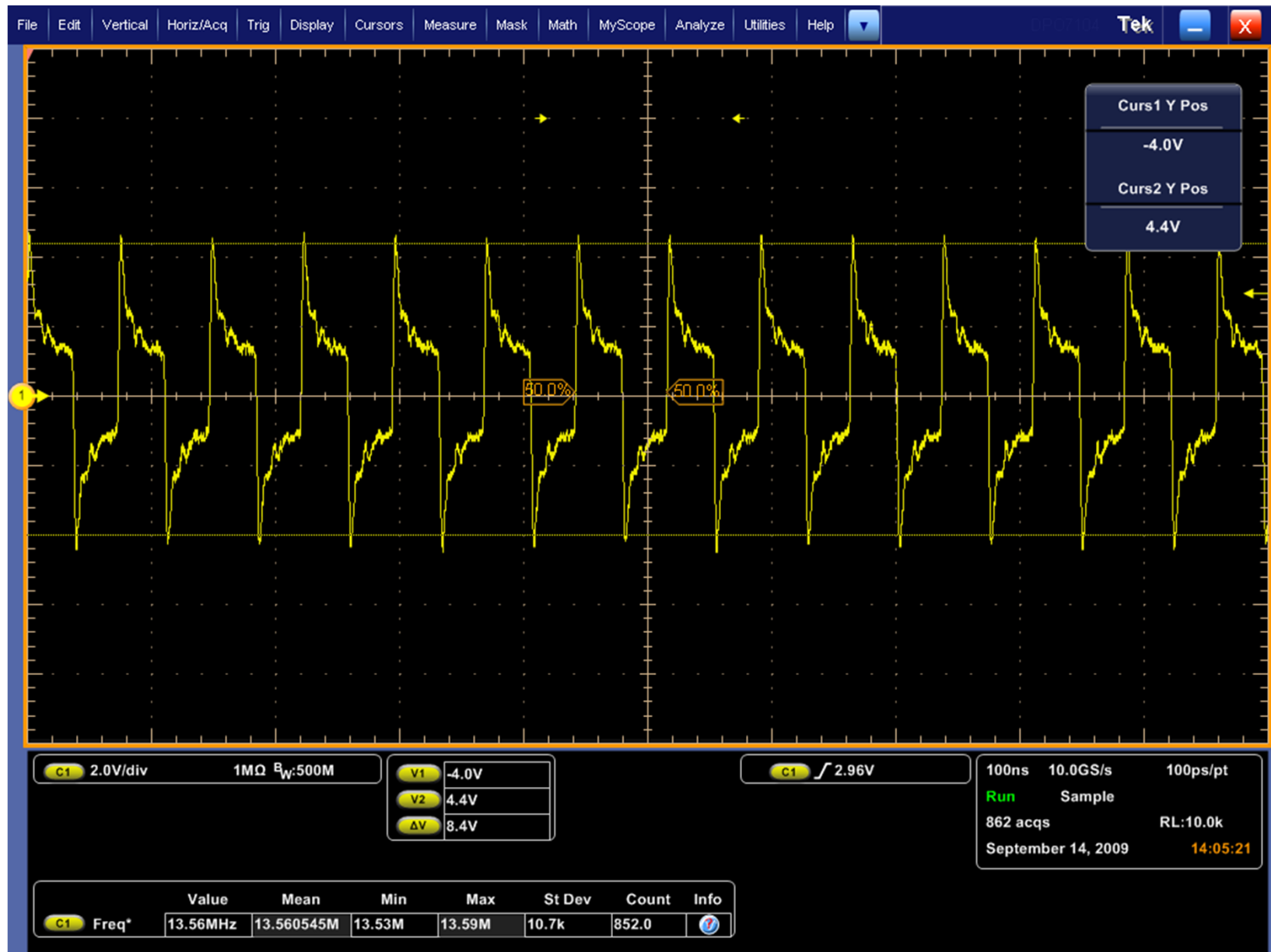
RF Test Points

- After the circuit has been constructed – we can then turn on the TX signal by writing register 0x00 with 0x21 and check the signal levels to confirm/correlate that component values and basic RF section of the circuit are OK.
- The following six slides are for reference to this check, but understand these signals are not absolute!
- These were captured from TRF79xx EVM, running at +5VDC In, with Full Power out setting.
- For those customers using different (lower) VIN, shapes of signals should be same, but will be lower level (although general ratio relationships should remain)

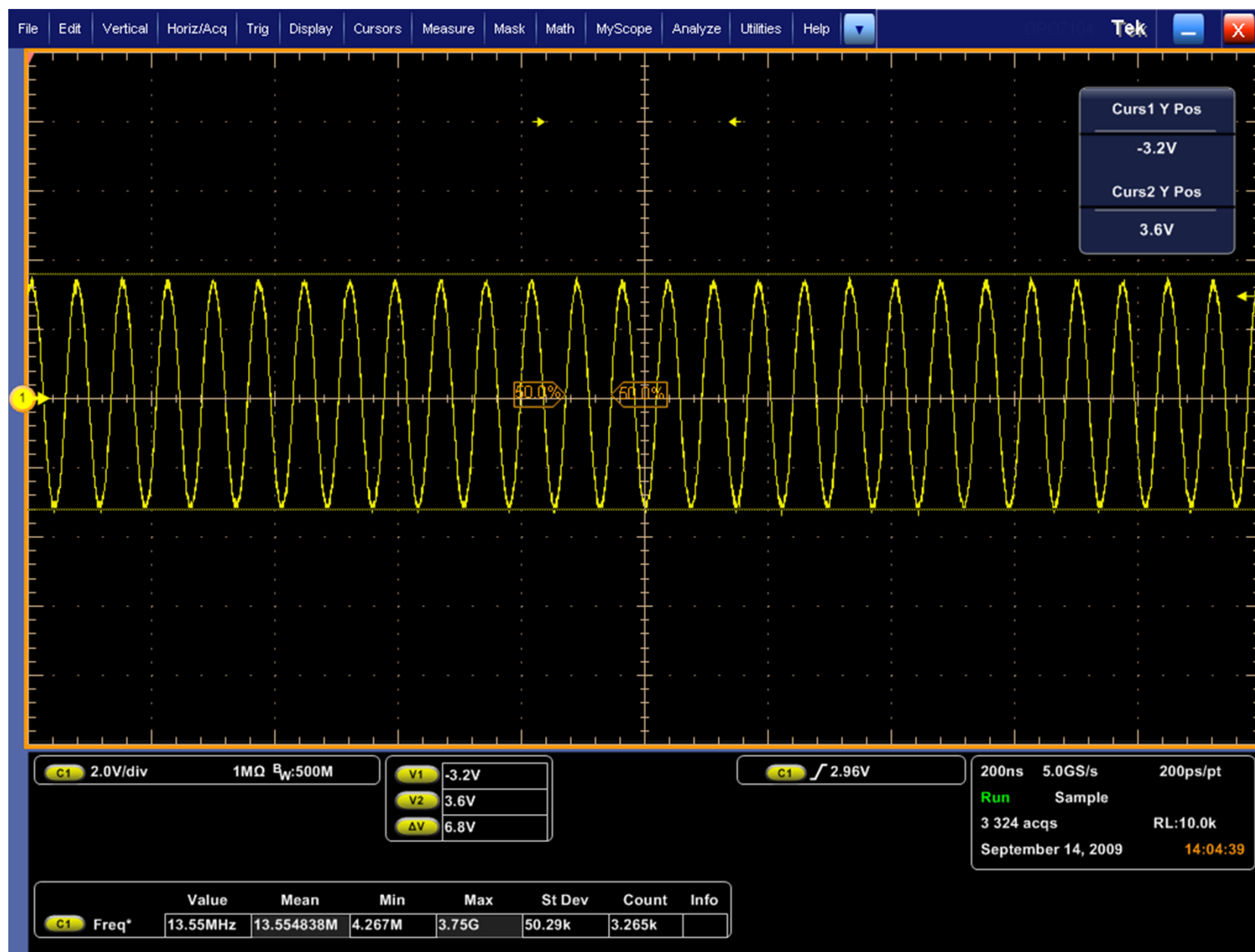
TRF79xx Pin 5 (TX_OUT)



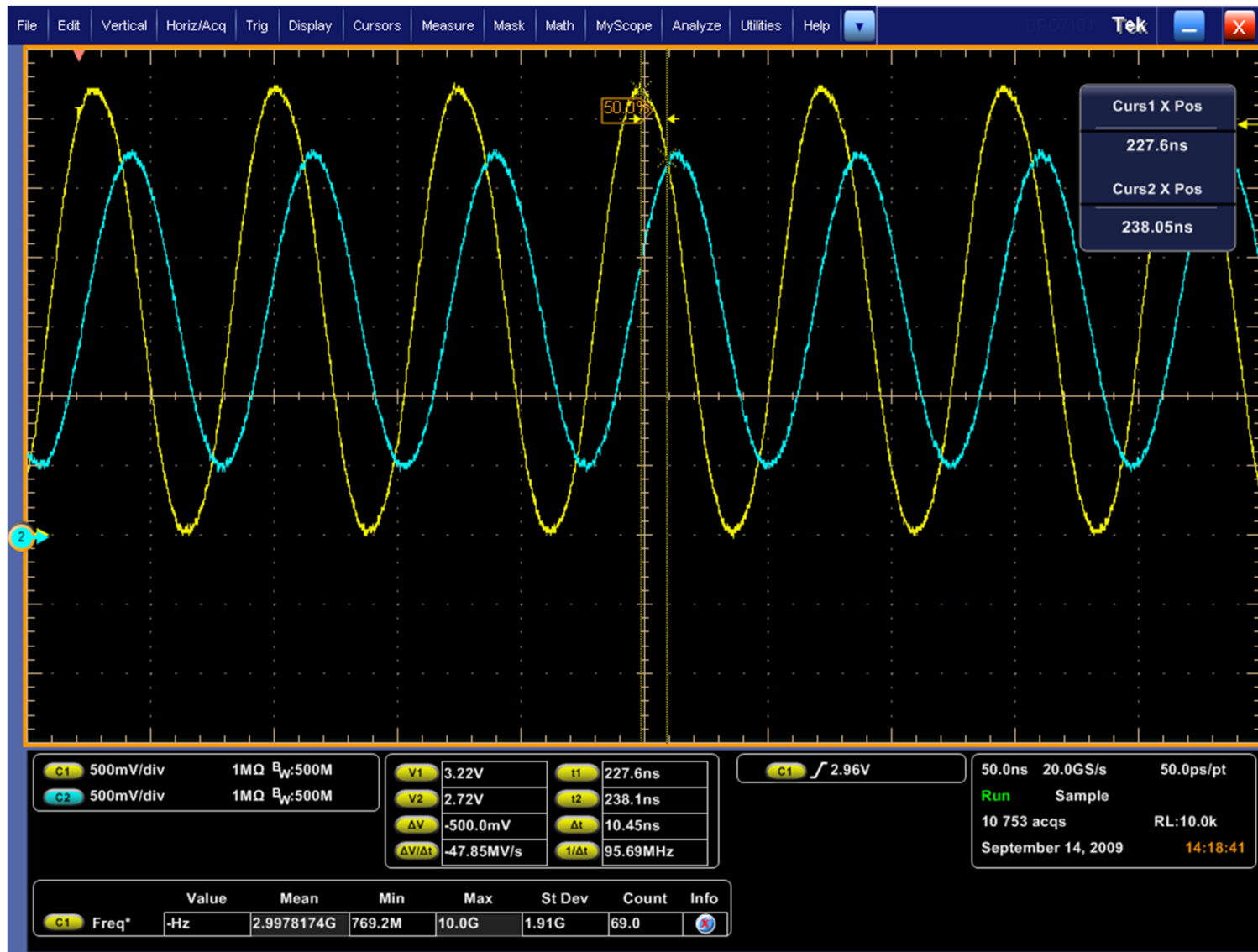
In-between DC Block Capacitors and L1



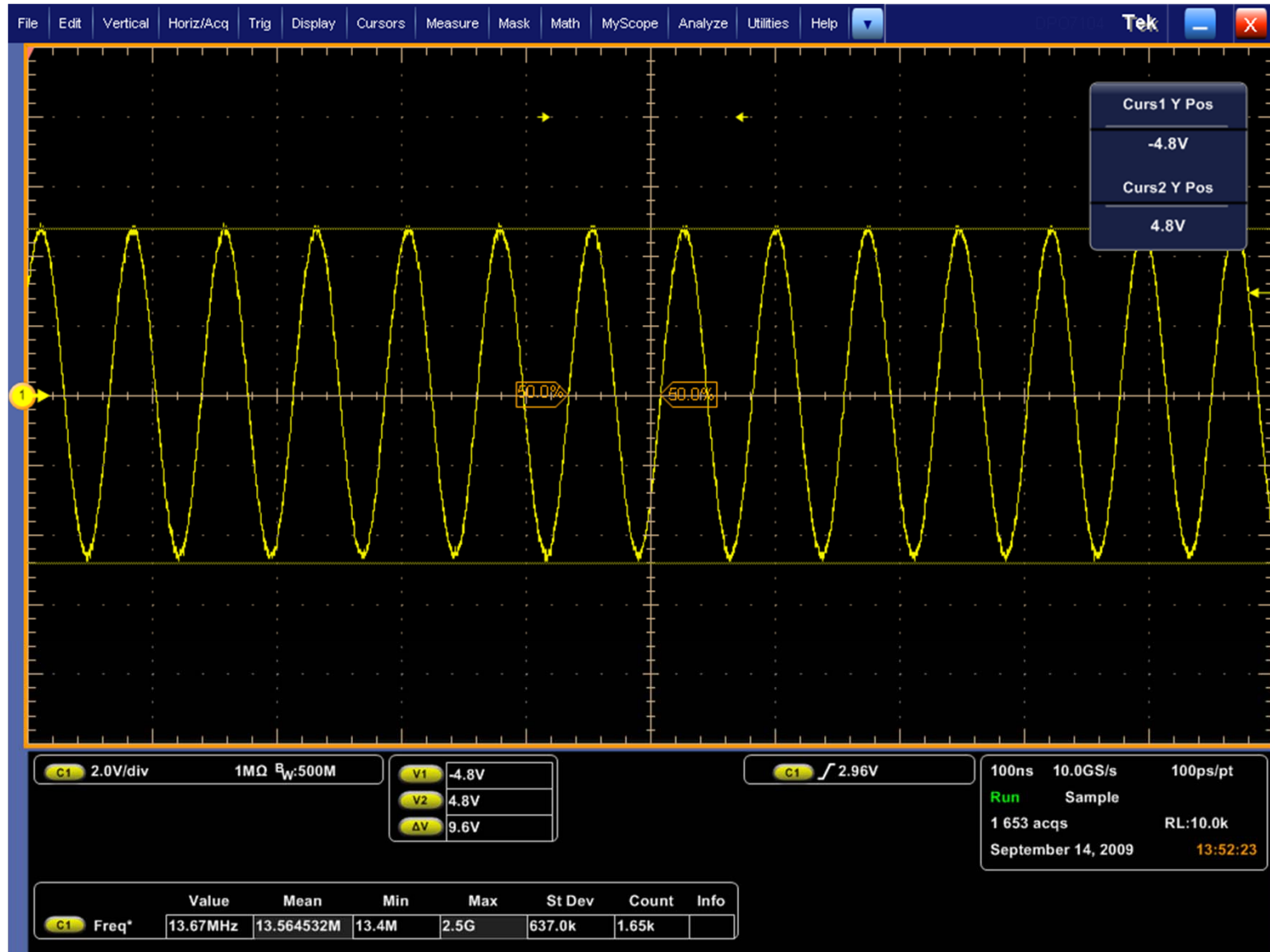
In-between L1 and L2



TRF79xx RX1_IN1 and RX2_IN2 (pin 8 = yellow & pin 9 = blue)

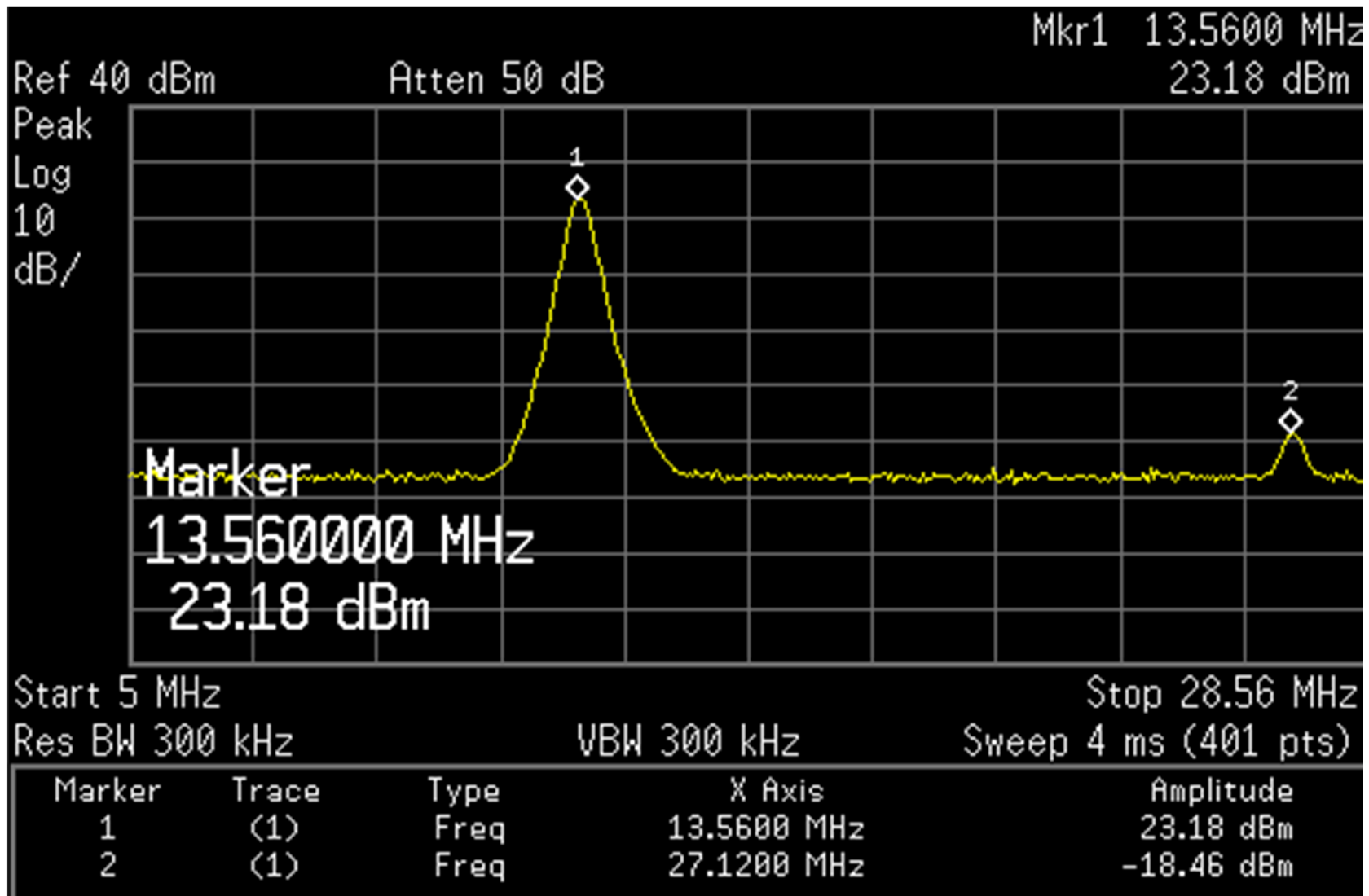


50 Ω Impedance Match Point (X2 or X3 RF Test Port)



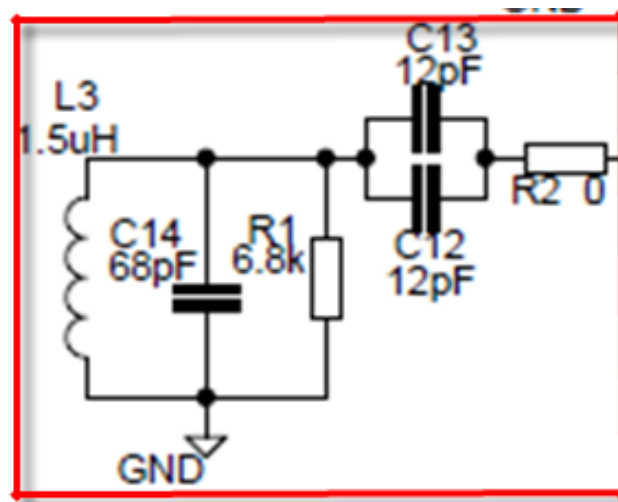
50Ω Impedance Match Point

Spectrum Analyzer Capture with Power Meter (showing fundamental and 2nd harmonic)



Antenna Impedance Match

- We now must make a matched 50Ω antenna (for full power transfer)
- This easiest way to do this is make the coil, calculate a parallel resistor $R_{(QDAMP)}$ and then express on a Smith Chart for verifying values, then moving to standard values available for low cost production worthy circuit.
- The section outlined in red is what we are discussing now. (Exact values are not important right at the moment.)



Antenna Impedance Match (cont.)

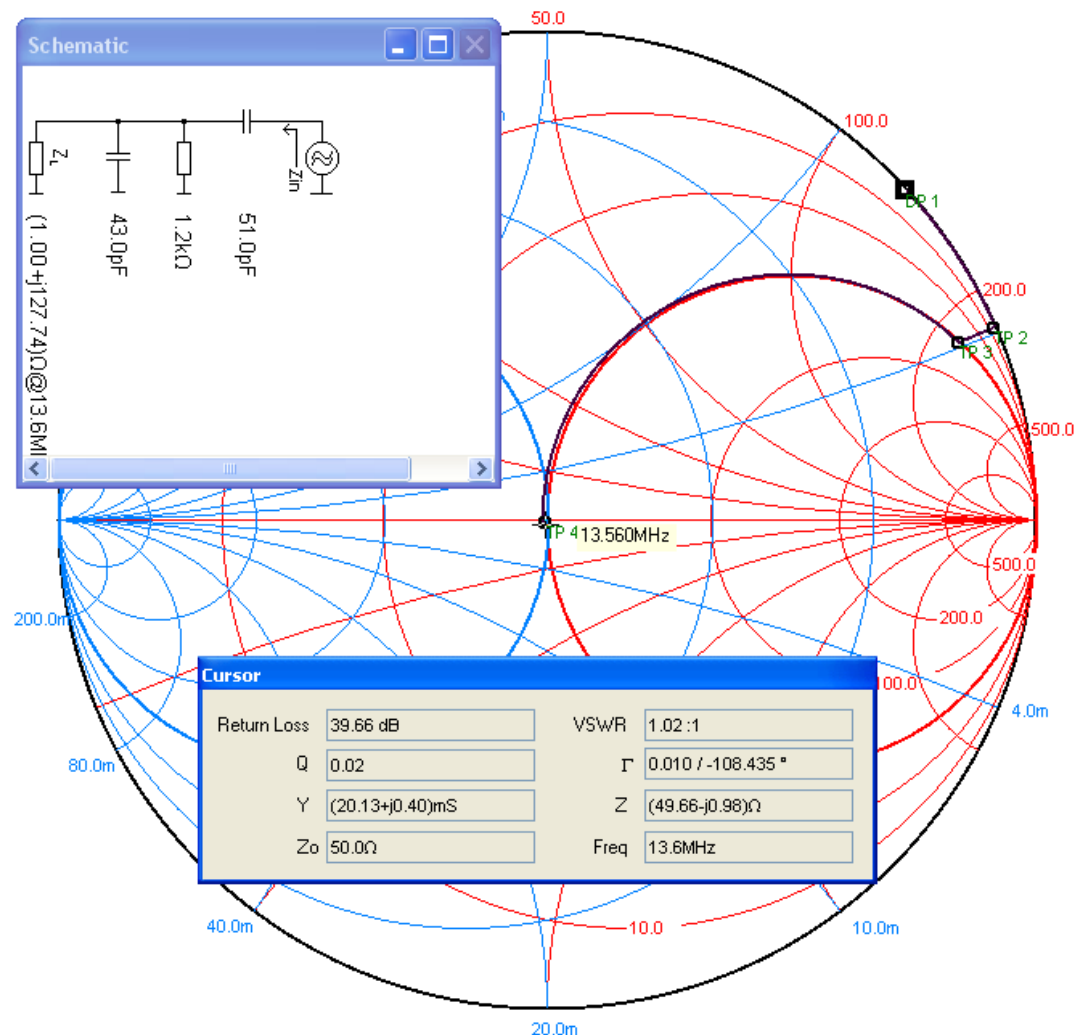
- Next we shall consider the antenna matching to the 50Ω point.
- In addition to making impedance match, we must also consider the resulting Q factor of the antenna circuit.
- For brevity in this presentation, usually two Q factors are considered for NFC or RFID antennas. $Q = 10$ and $Q = 20$.
- We also must consider that the coil inductance needs to be within a value range which allows tuning to 13.56MHz with standard value components.
- Again, due to time constraints – let us just know here that value of between 1uH to 2uH is a value to aim for when making PCB coil for NFC or RFID applications.
- Both Q and inductance value topics could take up much more time of course, but lets assume these targets and show an explanation and method for achieving success for the customers!

Antenna Impedance Match (cont.)

- Worked example:
 - First we shall calculate the parallel resistor ($R_{(QDAMP)}$) needed for a given inductance in order to control the Q factor of the tuned antenna.
 - Assume a coil inductance of 1.5uH (complex impedance = $1 + j127.735$)
 - Q target = 10
 - $R_{(QDAMP)} = 2\pi f L Q$
 - $R_{(QDAMP)} = 6.28 * 13.56\text{MHz} * 1.5\text{uH} * 10$
 - $R_{(QDAMP)} = 1.27\text{k}\Omega$
 - $R_{(QDAMP)} = 1.2\text{k}\Omega$ (move to a standard value)

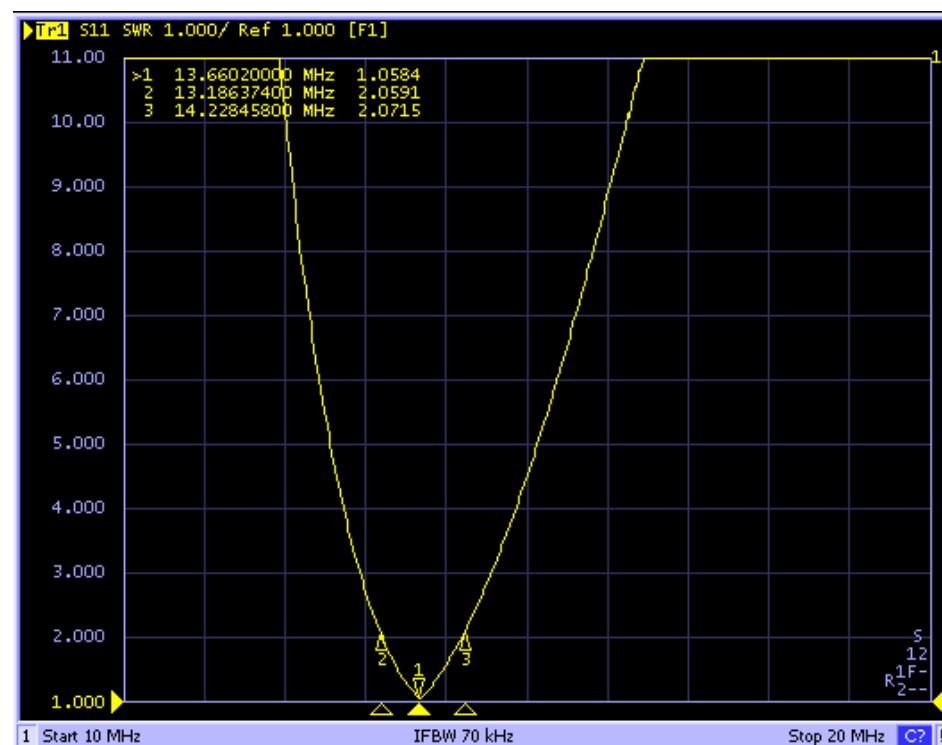
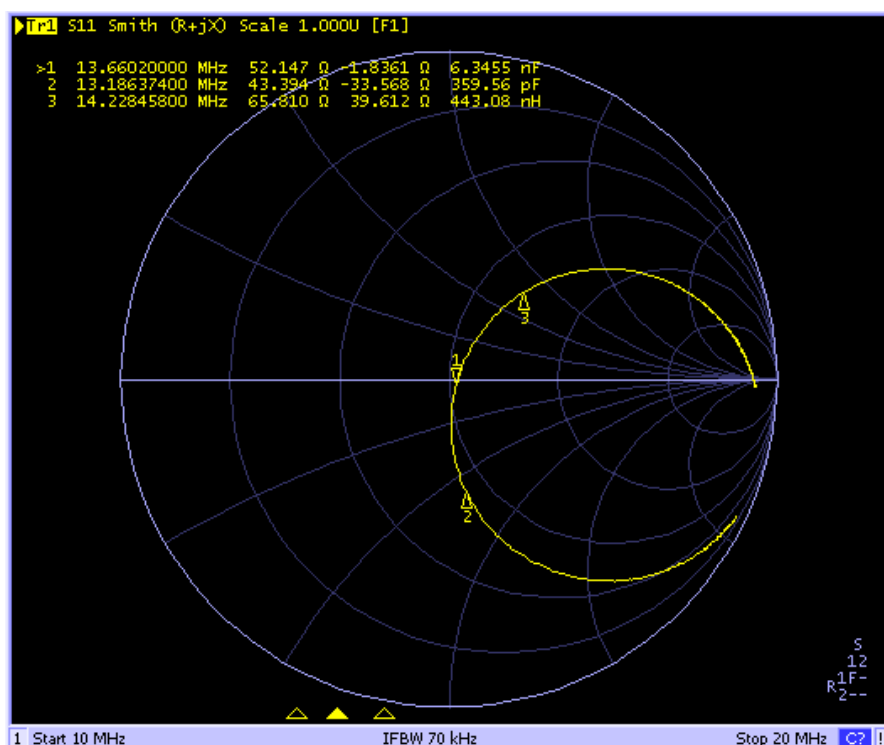
Antenna Impedance Match (cont.)

- Worked example:
 - Now we have calculated the complex impedance and we also know the resistor value needed to achieve the desired Q, we can move to simulation tool to get capacitor matching values very quickly.



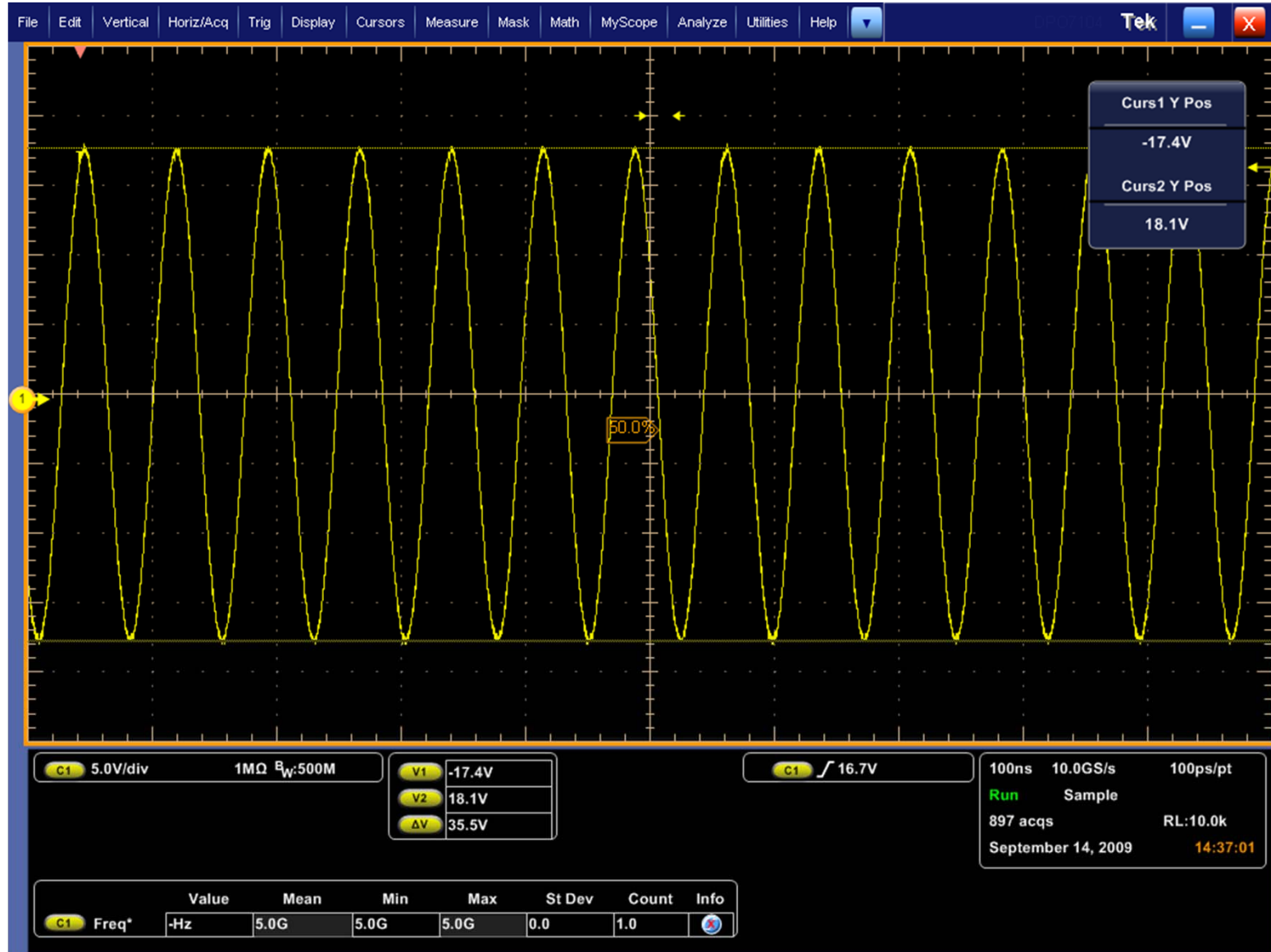
Antenna Impedance Match (cont.)

- Now we can populate the circuit and measure with the Network Analyzer to confirm our simulation with actual results.
- Below is Smith chart and SWR plot from NA, next slide is oscilloscope capture of the voltage on the tuned coil when powered by the TRF79xxA



Antenna Coil Signal

(Signal Level will vary with Q setting of the Antenna circuit)



NFC/RFID Applications driving new business

- Alternative Carrier Handover (Authentication/Pairing) for:
 - WiFi
 - Bluetooth/BLE
- High Security Card Access
 - Using MSP430 + Secure Element
- EMV Certification
 - Contactless Payments (Worldwide Requirement)

NFC Pairing Solution – TI’s “Tap and Pair”

NFC “Tap and Pair”

- **What is it?**
 - A Texas Instrument’s NFC Pairing solution
- **What are the Benefits?**
 - **Automated**
 - No user input - “Tap and Pair” process
 - **Instant**
 - Establishes WiFi connectivity in seconds
 - **Secure**
 - Establishes a secure BT or WiFi connection
 - **Ultra Low Power**
 - 3.5uA in card emulation mode
 - **Quick Time to Market**
 - Source Code and reference design available today



TI NFC application / reference designs

Bluetooth Connection and Pairing using NFC

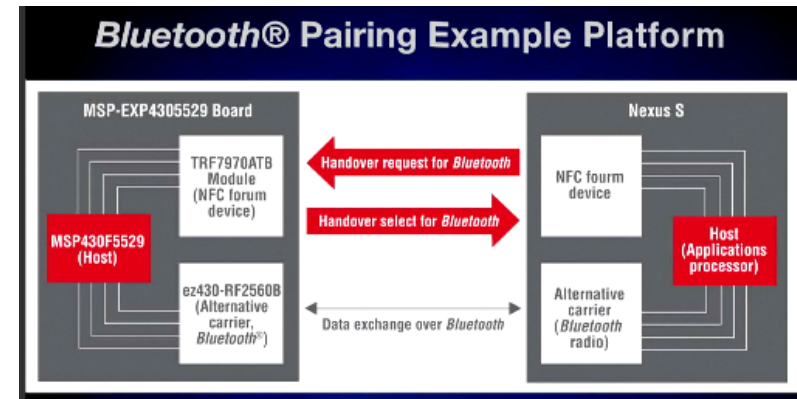
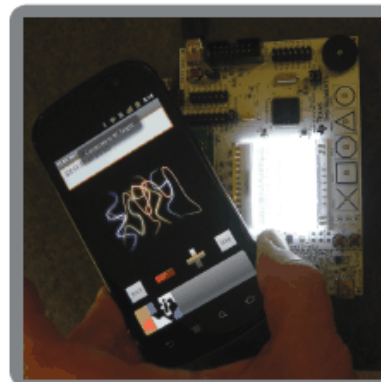


About

- Bluetooth SPP (Serial Port Profile) connection established automatically using NFC
- Works with Android NFC enabled smart phones
- SPP profile allows for bi-directional communication over the air interface

Benefits

- Simplifies Bluetooth pairing process
- Enables Bluetooth pairing of devices without user input (because of the usage of NFC)
- Source Code and reference design available for quick time to market



Video



http://focus.ti.com/general/docs/video/Portal.jsp?entryid=0_b7tnw1jl&lang=en

TI NFC application / reference designs

WiFi Configuration via NFC

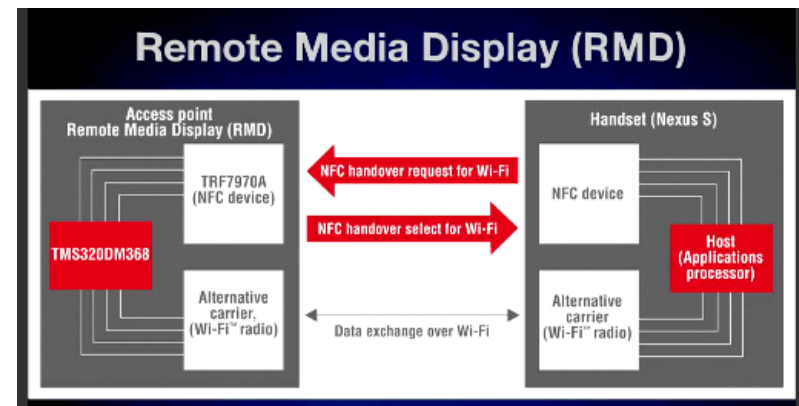


About

- WiFi connection established automatically using NFC
- Texas Instruments TRF7970A is set up in ISO14443B card emulation mode where the NDEF message contains the SSID of the access point
- Works with Android NFC enabled smart phones
- DLNA server is available to stream audio, video and pictures

Benefits

- WiFi network connection is very easy to use in this manner
- Texas Instruments TRF7970A NFC transceiver only consumes about 3.5uA in card emulation mode
- Source Code and reference design available for quick time to market

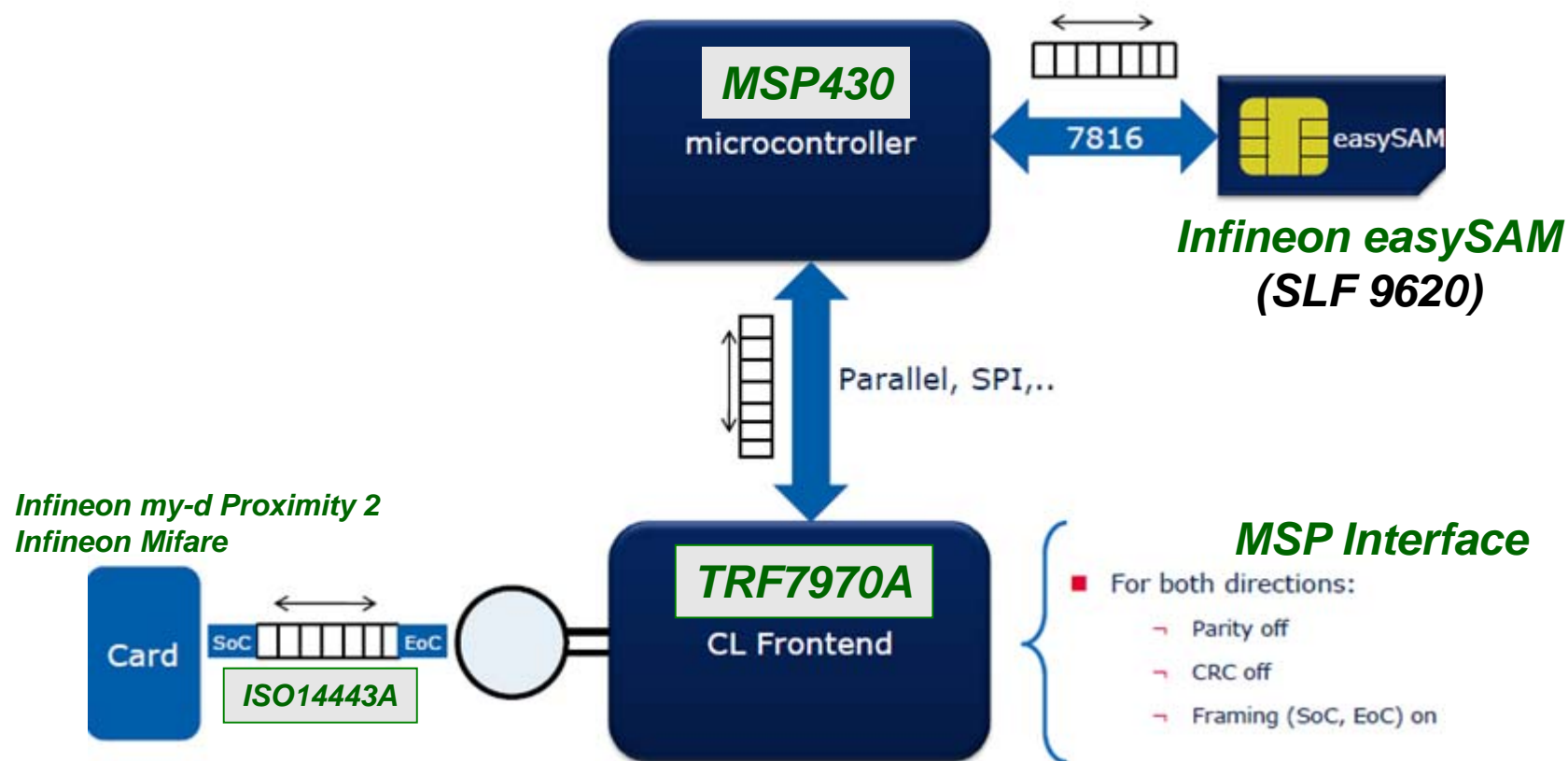


Video



http://focus.ti.com/general/docs/video/Portal.tsp?entryid=0_eu132zza&lang=en

NFC/RFID System using a Secure Element Block Diagram



ISO7816 Implementation

ISO7816 module description

Overview

This ISO7816 module implements the ISO7816 part 3 communication protocol between contact-based integrated chip circuit and readers.

Currently this module is implemented for prototype purposes. Therefore there are several limitations which have to take into account when re-using this module in other systems.

This document describes the implemented interfaces and functionality of the ISO7816 module as well the limitations.

Interfaces and their functionality

- `void Iso7816Init(void);`

This function initialized the GPIOs of the MSP430 microcontroller.

The GPIOs are defined as follows:

GPIO pin of MSP430F02370	Integrated Chip Circuit
P1.1	RST
P1.3	IO
P1.4	CLK

- `void Iso7816Atr(void);`

This function activates the integrated chip circuit. The ICC is sent a response to the microcontroller.

This first response is called Answer-to-reset (ATR).

Before activation a reset is initiated to allow activating the ICC via this function any time.

- `void Iso7816TxCmd(u08_t *, u16_t);`

This function transfers data to the ICC and waits for the response data.

The data which should be sent are enveloped according the T=1 protocol specification and a checksum is added.

Each individual byte are separated into 10 bit (1 start bit, 8 data bits, 1 parity bit) and a specified guard time after each 10bits.

Verse vice in the reception state all the bits are combined into a byte and then copied into an TX buffer.

Current limitation

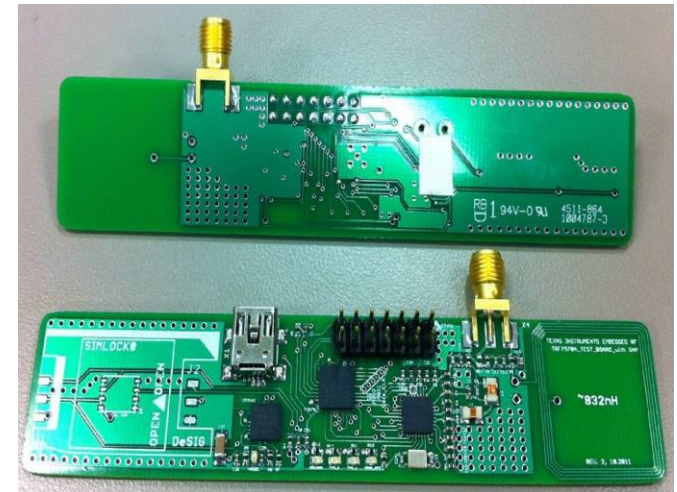
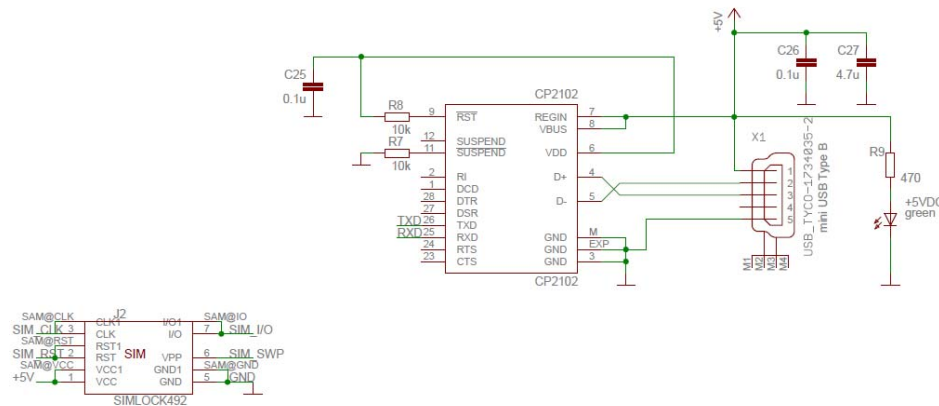
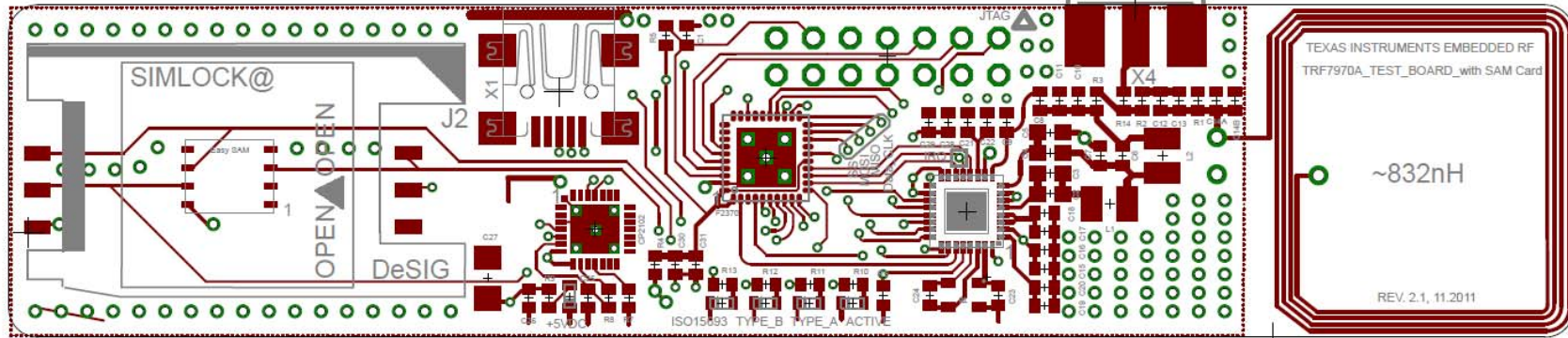
There are several limitations of the current implemented ISO7816 module.

- ATR
Currently only the activation of the Infineon "EasySAM" was implemented and tested. The dynamic interpretation of the received ATR is not supported. As the length of the ATR is fixed to 24 Bytes all other ICC which does not have identical ATR lengths will not work properly.
- T=1
The current module supports the T=1 protocol without any error handling for the communication (R-block handling). S-blocks are not supported.
- T=0
The current implementation does not support the T=0 protocol.
- PPS / Baud rate
PPS commands are not implemented. Therefore the baud rate setting is limited to the transmission factors F=372 and D=1.

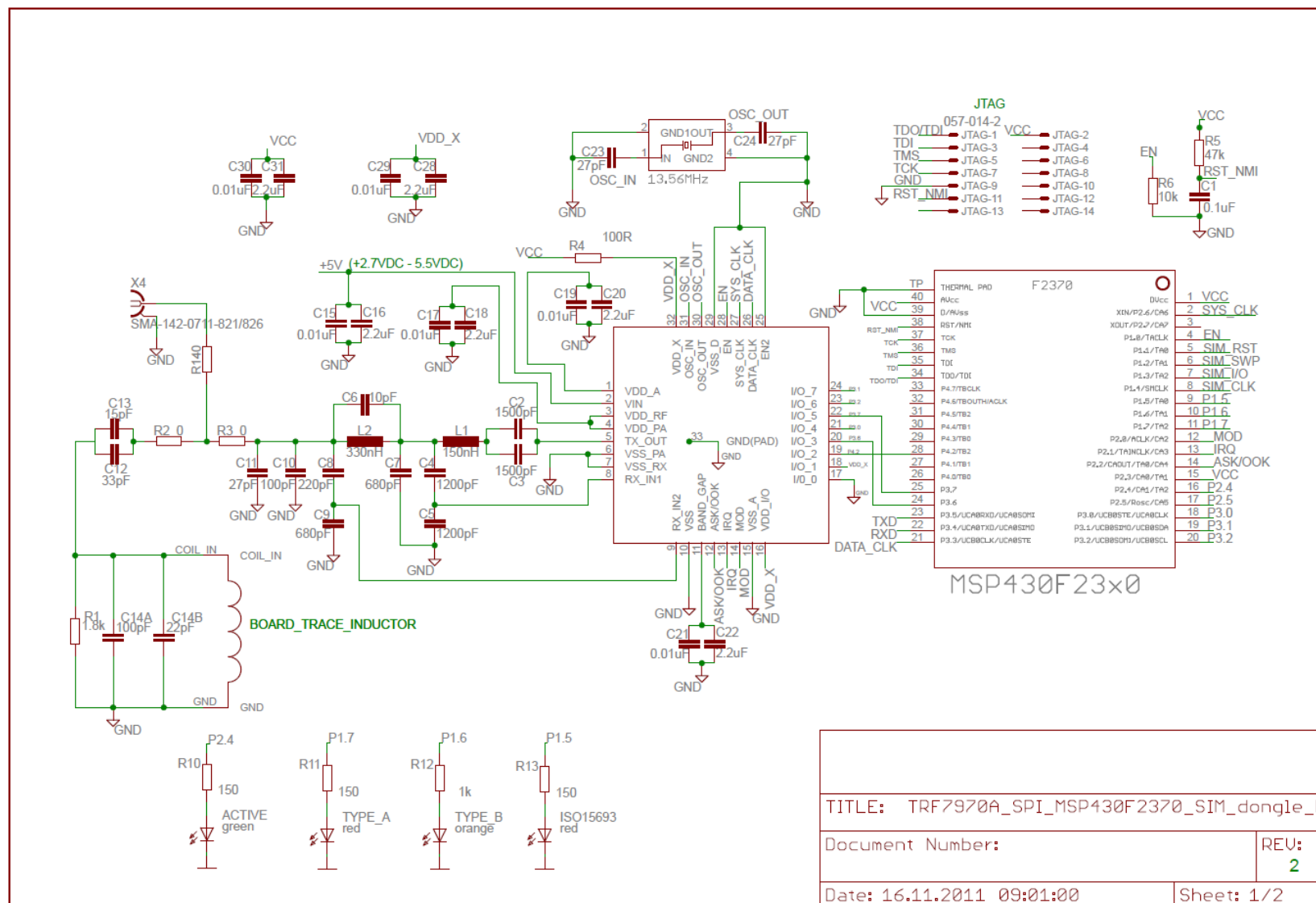
Next steps

- ATR
In order to support a more extensive set of ICC variants the ATR should be interpreted dynamically at their reception. If the ICC does not support the current implementation an appropriate output shall be given.
- T=1
R-Blocks for the detection of communication errors and S-blocks for configuration settings shall be implemented.
- PPS
In order to support a higher communication speed between the ICC and the reader PPS command shall be implemented.
- (T=0)
Optionally if necessary the support of the T=0 protocol may be implemented.

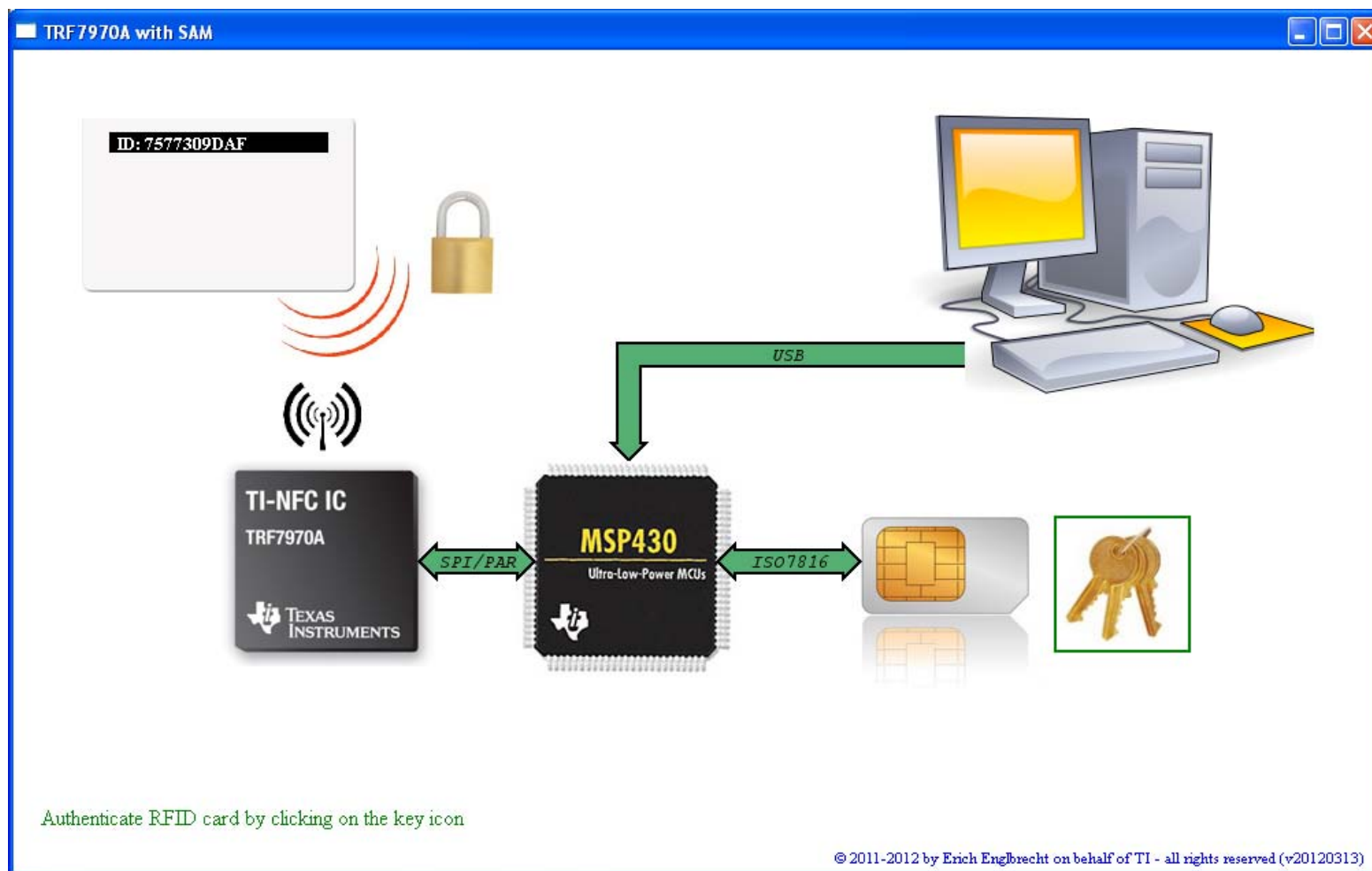
Circuit & Layout V 2.1



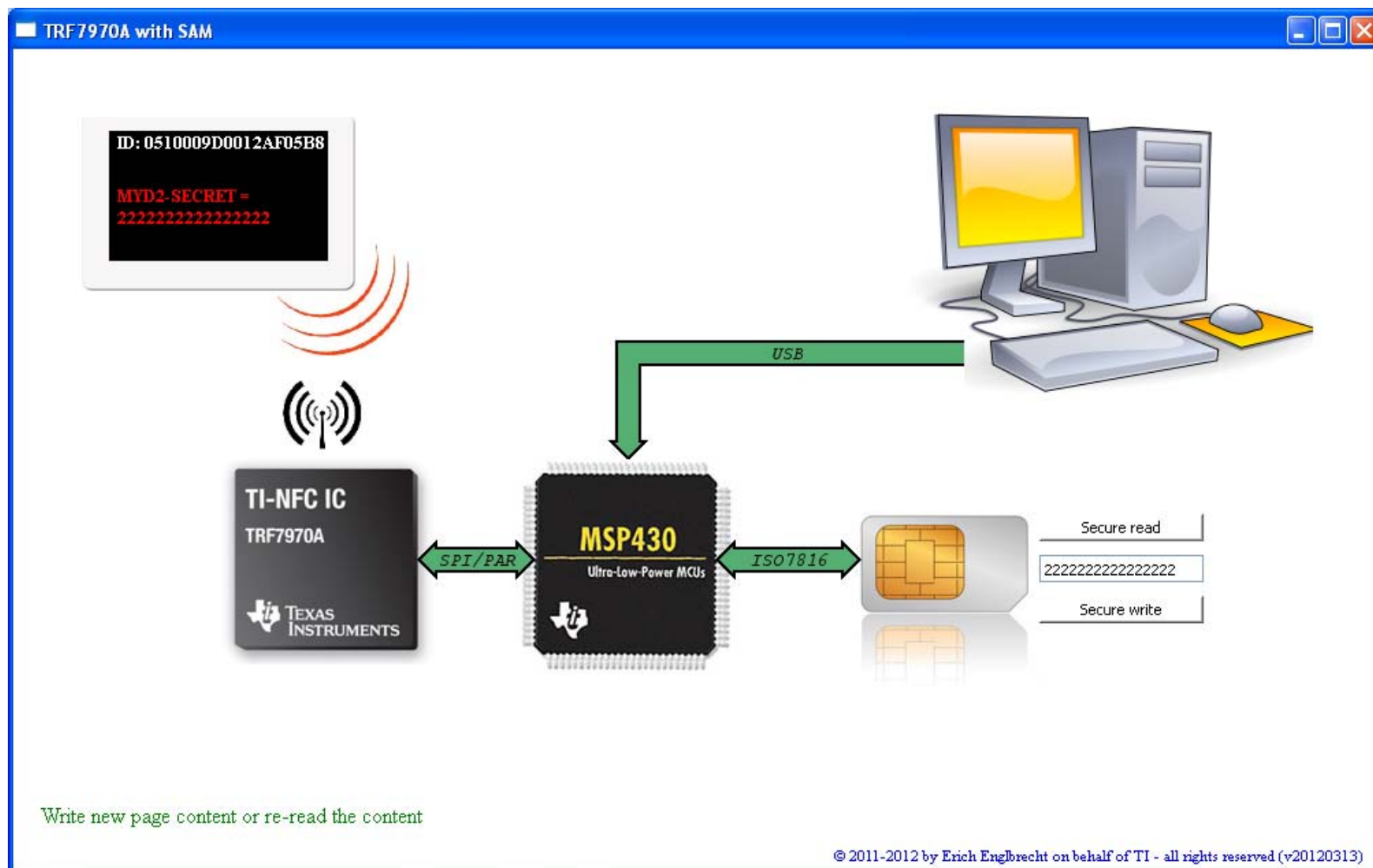
Circuit V 2.1



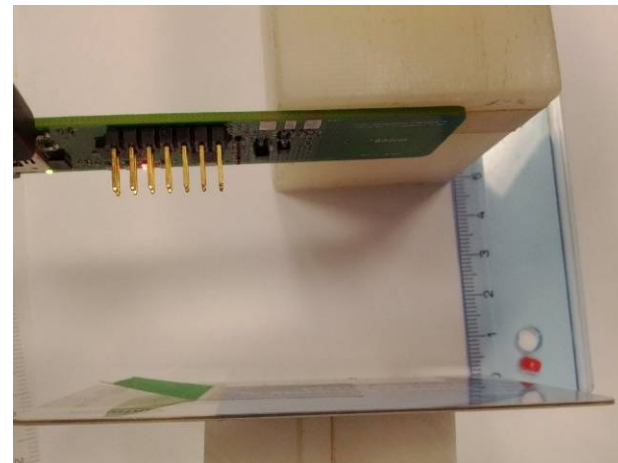
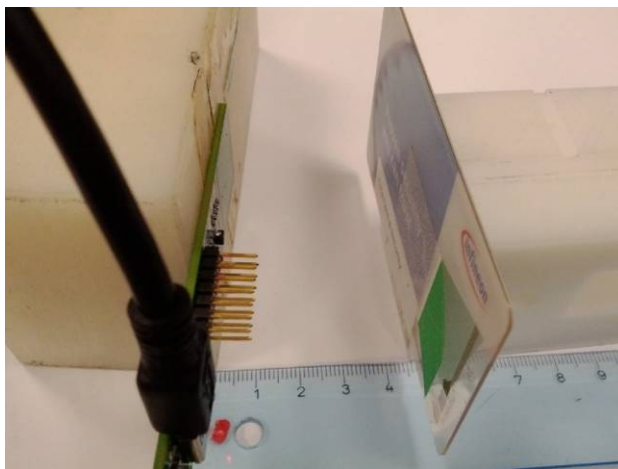
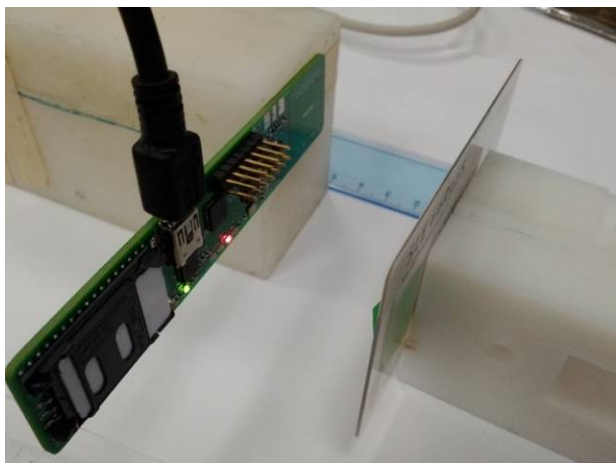
Demo GUI



Demo GUI



Performance



Reader Internal antenna

Infineon`n **my-d prox2 SLE66R32S**

Tag detection **4.5cm**

Auth+ write= **3cm**

Mifare ..DAF

Tag detection=4cm

Auth+ write=3cm

Mifare ..D5F

Tag detection=4cm

Auth+ write=2.5cm

Reader ext antenna 5x5cm

Infineon **my-d prox2**

SLE66R32S

Tag detection **7.5cm**

Auth+ write=**6cm**

Mifare ..DAF

Tag detection=7.5cm

Auth+ write=5.5cm

Mifare ..D5F

Tag detection=7.5cm

Auth+ write=5.2cm



EMVL1 Analog Compliance Testing Overview and status with TRF79xxA

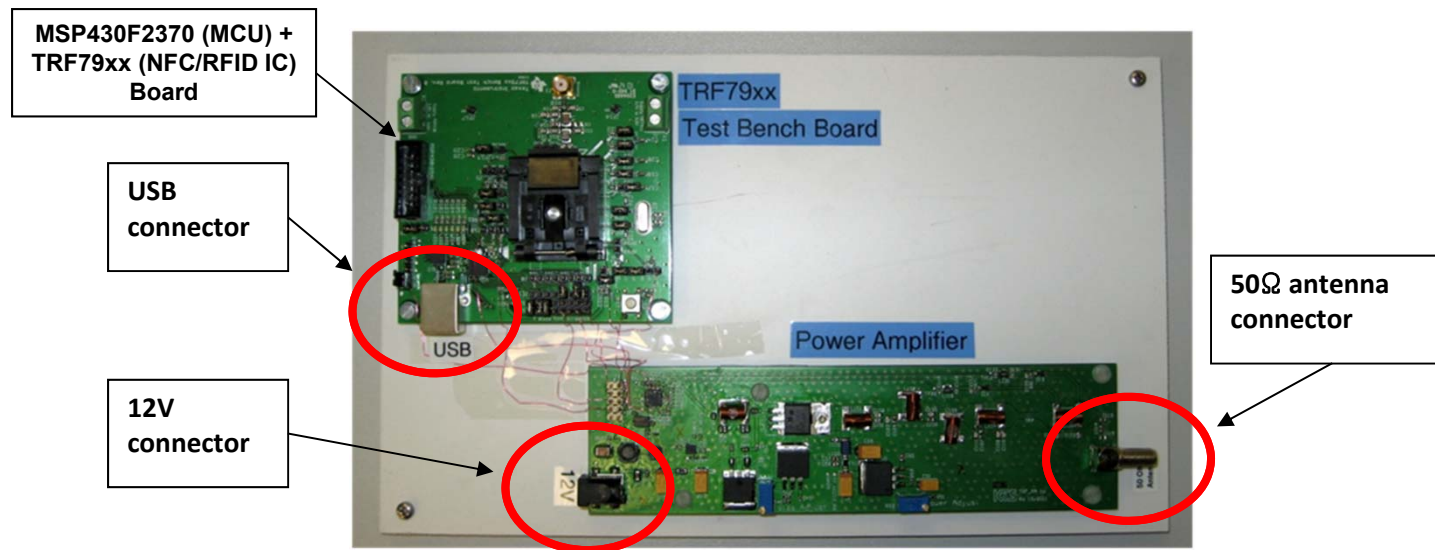
Embedded RF
Applications/Systems
04/2012

High Level Summary of EMVL1 Requirements

- EMV Contactless Communication Protocol Specification
 - current version is 2.1 (dated March 2011 and November 2011)
- EMVL1 Analog testing consists of measuring:
 - ✓ Un-modulated PCD Power (as measured by EMV Test PICC, section 3.2.1)
 - ✓ PCD Carrier Frequency (as measured by EMV Test PICC , section 3.2.4)
 - ✓ Reset of the PCD Operating Field (as measured by EMV Test PICC , section 3.2.6)
 - ✓ Modulated PCD Field (mod depth, as measured by EMV Test PICC, for ISO14443 Types A&B, section 3.3)
 - ✓ PCD Receiver Quality (as measured by EMV Test PICC using various levels of load modulation, section 3.4)
 - ✓ Synchronization (as measured by EMV Test PICC, ISO14443B only, Section 4.3)
 - ✓ Bit Coding (Section 4.4)
 - ✓ Symbol Synchronization (Section 4.5)
 - ✓ De-Synchronization (Section 4.6)
 - ✓ Frame Size (as measured by EMV Test PICC, Section 4.7)
 - ✓ Command Frame Timing (Section 4.8)
 - ✓ Type A Command Set (Section 5)
 - ✓ Type B Command Set (Section 6)
 - ✓ Polling (Section 9)
- EMVL1 Digital testing consists of:
 - Half Duplex Block Transmission Protocol (Section 10)
 - o Layer 4 commands
 - o Chaining
 - o Exception Processing

EMVL1 Analog Test Setup w/ Power Amplifier Module

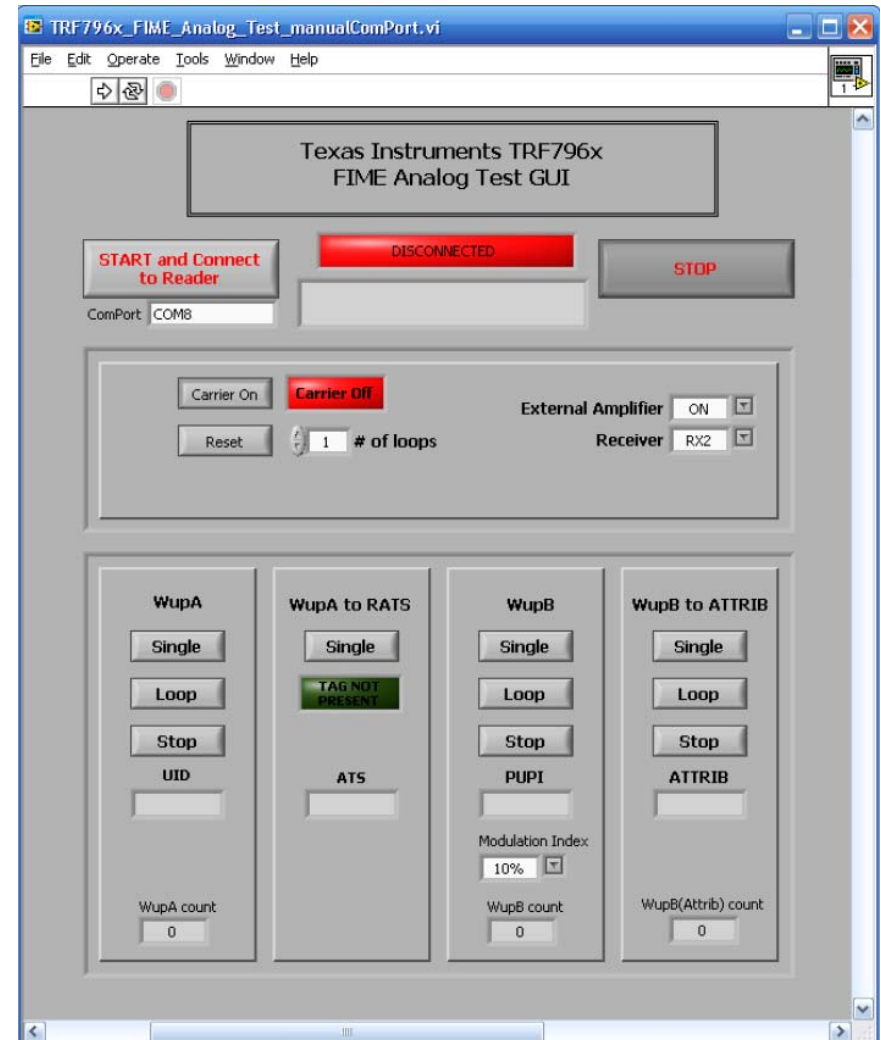
- Because of the EMVL1 PCD to PICC power transfer test requirements (this is the most difficult part of the test), a **prototype** 1W power amplifier for the TRF79xx was created for investigating the amount of power that would be required using the smaller antenna size (as compared to what is in ISO10373-6) specified in the EMVL1 documents.
- Key points that were considered in this design were to pass EMVL1 **and** EMC regulations.



**Customer and TI
Antennas used**

EMVL1 Analog Test GUI

- EMVL1 Test GUI which acts as 'host' to TRF79xxA module was created for test efforts at FIME/Applus (EMV test houses)
- This GUI was created to conform to the EMVCo Type Approval Contactless Terminal Level 1 Device Test Environment Specification, v2.0.1a.
- This GUI is only made for EMVL1 Analog testing at the moment. EMVL1 Digital section can be added with some additional effort.

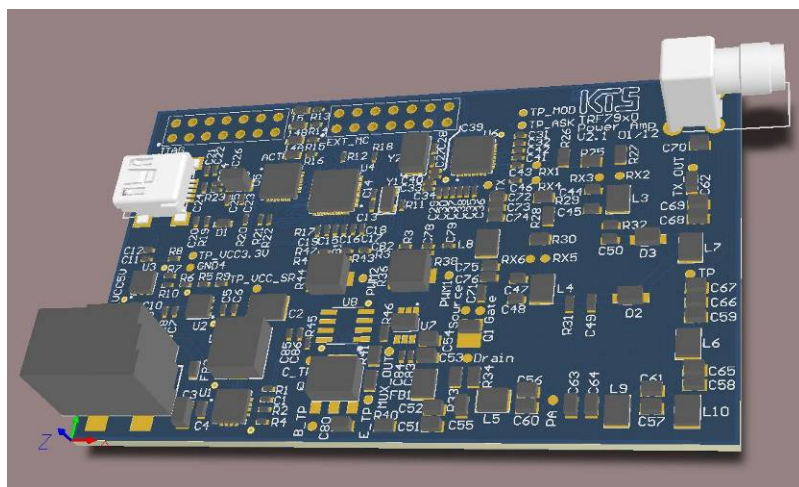


Texas Instruments EMVco L1 Pre-Test Summary

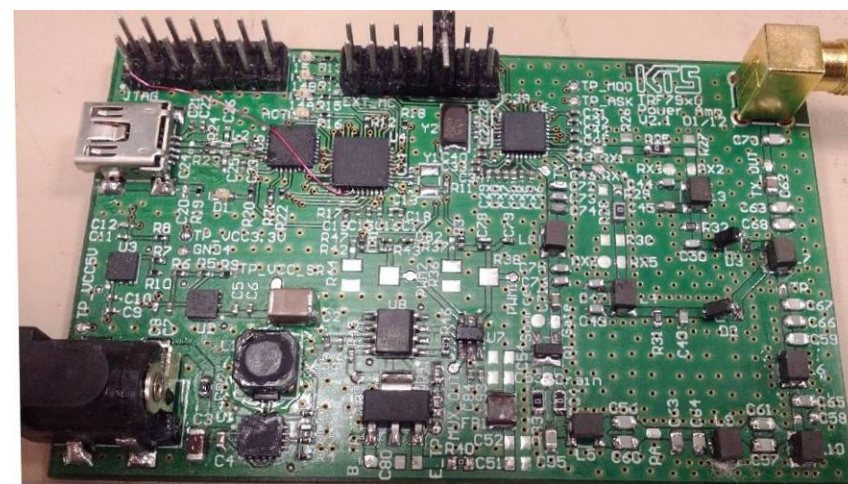
- EMV Contactless Communication Protocol Specification
 - For this test, EMV Contactless Communication Protocol Specification V: 2.0.1
 - current version is 2.1 (dated March 2011 and November 2011)
- Pre-Test Purpose:
 - EMVL1 Radio Frequency Power Compliance Testing
 - **NOTE:** At the time of this pretest, the version of the amplified reader did not support 10% modulation depth (for ISO14443B), so the test was executed only for ISO14443 Type A.
- Test Section Results:
 - 3.2.1 : Pass
 - 3.2.3: N/A
 - 3.2.4: Pass
 - 3.3.2: Pass
- Conclusion:
 - With the given output power and a customer antenna, the analog tests can be passed. The official testing on the 10% modulation will be done in next several weeks. (see next slides for new board and preview lab measurements!)

Next generation of the TRF79xx w/Power Amplifier (04/2012)

- New board layout was created which integrates the MCU, the TRF79xx and the power amplifier, all on one module which is made with POS vendor potential size/space requirements in mind.
- Modulation depth control will be handled by MCU and fixed resistor arrangement.
- Board could be shrunk further by customers by integrating host communication interface (removal of USB), integrating with other MCU (perhaps already in place, i.e. Sitara, Stellaris, etc.)



CAD Drawing of newest version of Amplifier Board.
(dimensions are 8cm x 5cm)



Populated version of Amplifier Board

Type A Pause Measurements

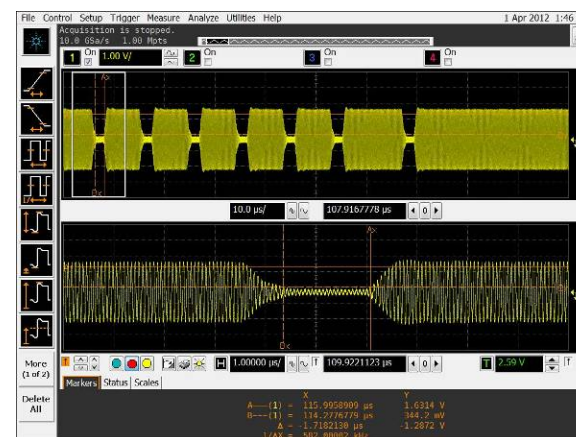
- Type A Pause measurement requirement is for T1-T4 timings to be met.
- Below are screen captures from these measurements on the TI based EMVL1 design.



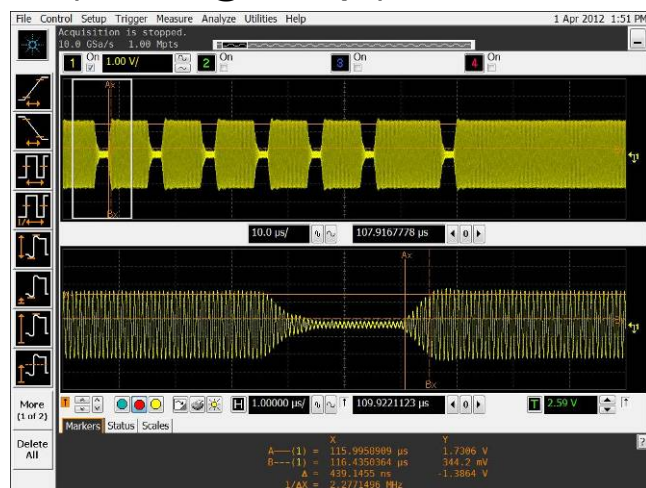
Overall (T1 + T3, @ 106kbps)



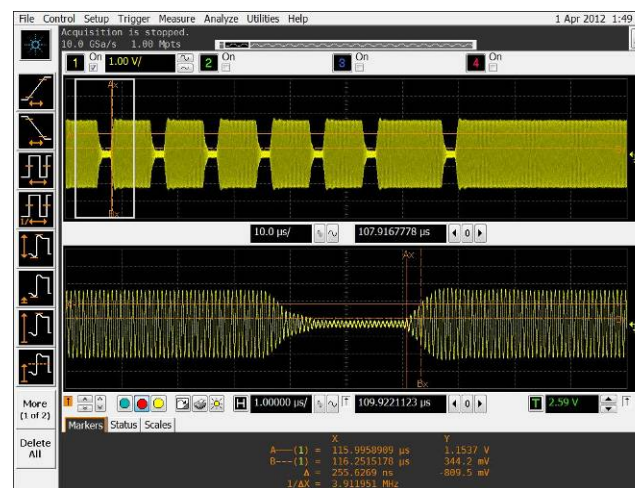
T1



T2



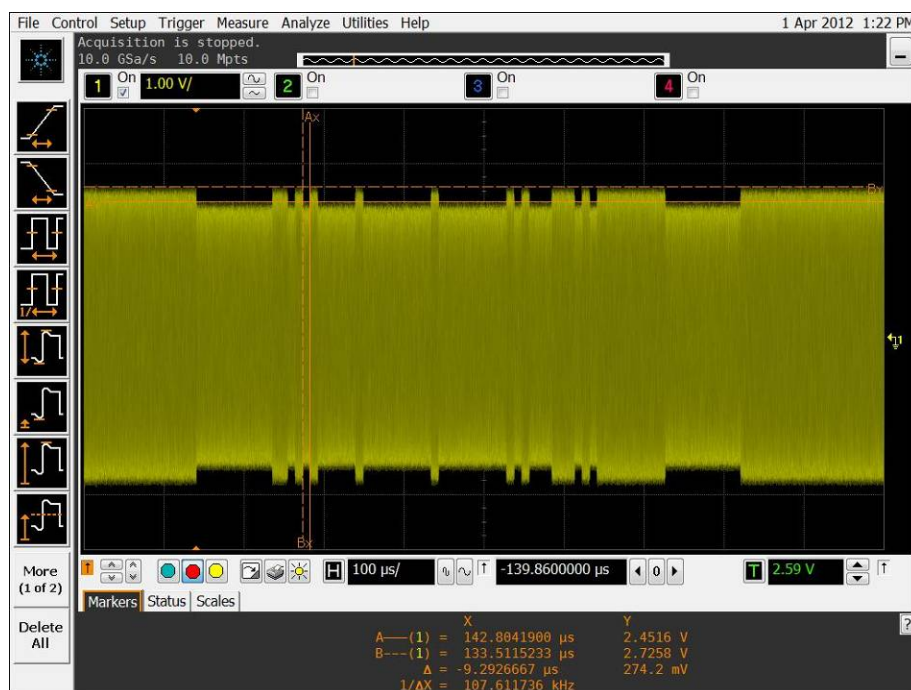
T3



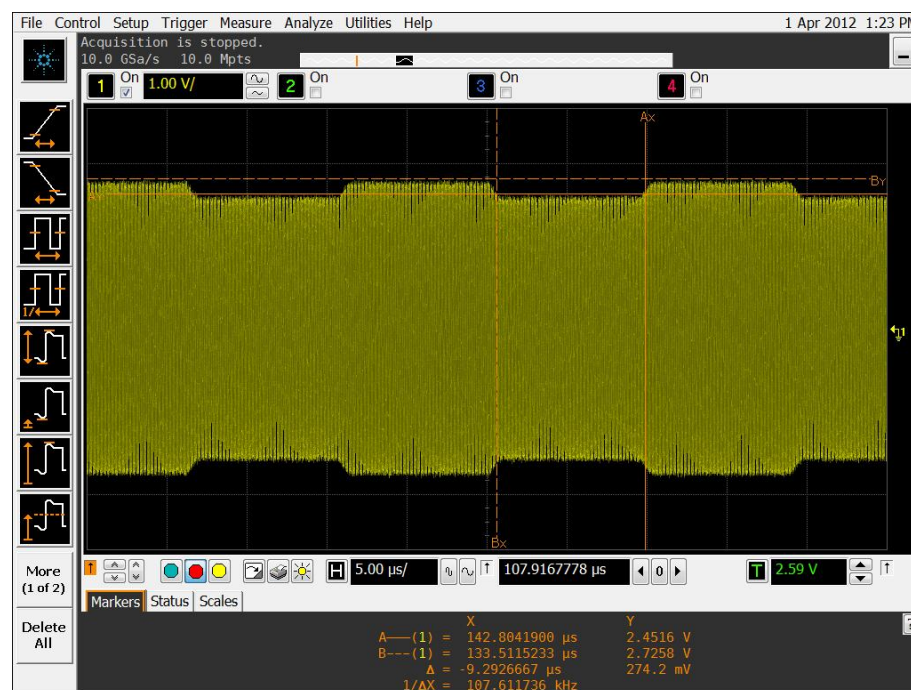
T4

Type B Modulation Depth

- Design has been measured to meet 10% modulation depth requirements for ISO/EMVL1
- Below are screen captures from these measurements on the TI based EMVL1 design.



**ISO14443B, 10% Modulation
Depth Overall Capture**



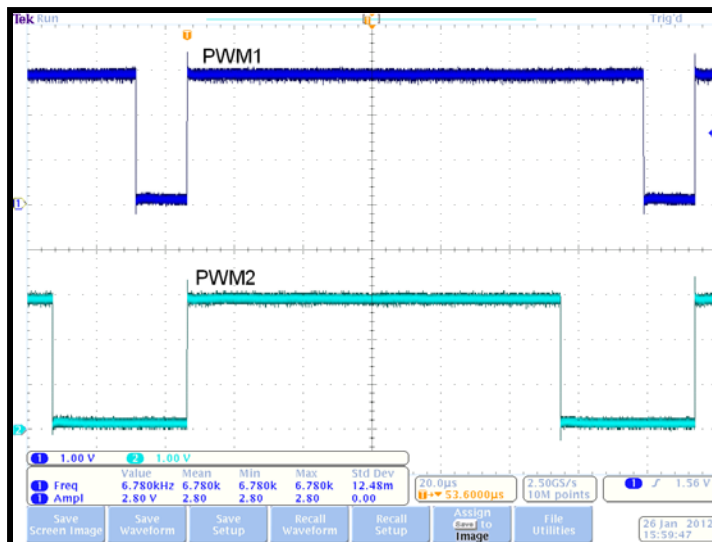
**ISO14443B, 10% Modulation
Depth Zoom**

Backup

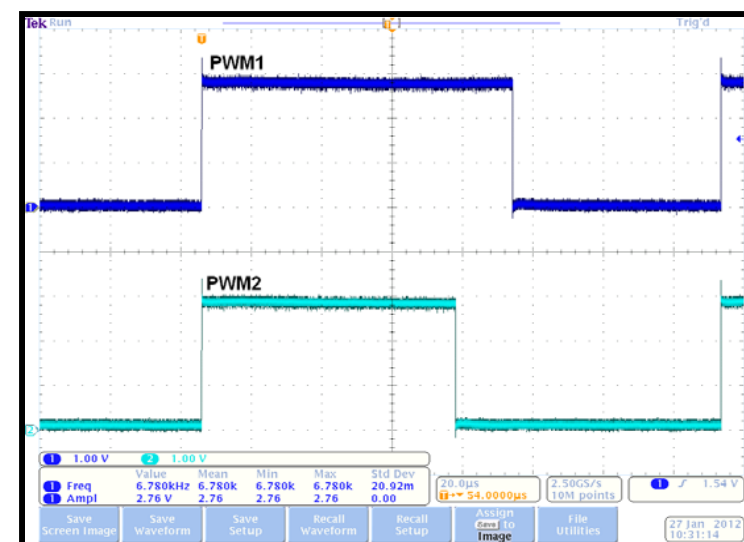
- PWM approach for modulation depth control and system noise control (if needed)
- technical steps for EMVL1 testing

2nd generation of the TRF79xx w/Power Amplifier (04/2012)

- As previously noted, the original amplifier prototype was limited to ISO14443A modulation depth (100%). This was due to a lack of precise control in that hardware of the 10% modulation depth of the carrier required for ISO14443B.
- New design will implement this control using firmware and TimerB (two PWM outputs) on the MSP430 for accurate control (as shown below) and a second order filter for clean signal.
- This new design will also have adjustable power out, as it was found that 1W was too much power for EMVL1 compliance.



Measured Duty Cycle of PWM1 is 89.86% and of PWM2 is 72.97%. The modulation depth is 10.37%.



Measured Duty Cycle of PWM1 is 59.8% and PWM2 is 48.9% to hold modulation level, which is 10.1%.

Un-modulated PCD Power (section 3.2.1)

- The power delivered by the PCD is measured on the EMV TEST PICC.
- The value of the power level measured on the EMV – TEST PICC must fall within range.
- Reference ~7cm diameter PCD antenna is used (not ISO10373-6, -7 antenna)
- From Table 3.2—Measurement of Power Transfer PCD to PICC (**PCD Transmission**)
 1. Activate the PCD to emit the carrier without any modulation by using the PCD Test Environment as described in Annex B.4.
 2. Place the EMV – TEST PICC in the Operating Volume of the PCD. Apply no modulation to J2 of the EMV – TEST PICC. Configure the EMV – TEST PICC with non linear load.
 3. Measure the mean value of the voltage at J1 of the EMV – TEST PICC.
 4. Within the Operating Volume, the PCD shall generate a voltage V_{OV} at J1 of the EMV – TEST PICC. The voltage V_{OV} shall be measured as described in Table 3.2. Refer to Annex A.2 for the value of V_{OV} .

from Annex A.2 (Table A.2)

Topic	Parameter	Value		Units
		Min	Max	
Power Transfer PCD→PICC	$V_{OV} (0 \leq z \leq 2)$	$3.10 - 0.05 z$	8.2	V
	$V_{OV} (2 < z \leq 4)$	$3.45 - 0.225 z$	8.2	V
	ΔV_{OV}	0	0.7	V
	$V_{OV,RESET}$	0	3.5	mV

Carrier Frequency Measurement of PCD (section 3.2.4)

- The carrier frequency generated by the PCD is measured on the EMV TEST PICC.
- The carrier frequency measured on the EMV – TEST PICC must fall within range.
- Reference ~7cm diameter PCD antenna is used (not ISO10373-6, -7 antenna)
- From Table 3.5 — Measurement of Carrier Frequency f_c (PCD Transmission)
 1. Activate the PCD to emit the carrier without any modulation by using the PCD Test Environment as described in Annex B.4.
 2. Place the EMV – TEST PICC in the Operating Volume of the PCD. Apply no modulation to J2 of the EMV – TEST PICC. Configure the EMV – TEST PICC with non linear load.
 3. Capture the signal at the output of the pickup coil of the EMV – TEST PICC and measure the frequency of the carrier.
 4. The frequency of the Operating Field (carrier frequency) provided by the PCD shall be f_c . The frequency shall be measured as described in Table 3.5. Refer to Annex A.2 for the value of f_c .

from Annex A.2 (Table A.2)

Topic	Parameter	Value		Units
		Min	Max	
Carrier Frequency	f_c	13.553	13.567	MHz

Reset of PCD Operating Field (section 3.2.6)

- The PCD must reset the operating field in a specific manner.
- The field reset as measured on the EMV – TEST PICC must fall within range.
- Reference ~7cm diameter PCD antenna is used (not ISO10373-6, -7 antenna)
- From Table 3.7—Measurement of Power Transfer PCD to PICC (PCD Transmission)
 1. Activate the PCD to emit the carrier without any modulation by using the PCD Test Environment as described in Annex B.4.
 2. Place the EMV – TEST PICC in the Operating Volume of the PCD. Apply no modulation to J2 of the EMV – TEST PICC. Configure the EMV – TEST PICC with non linear load.
 3. Capture the signal at the output of the pickup coil of the EMV – TEST PICC from the start until the end of the reset.
 4. When the PCD resets the Operating Field, then within the Operating Volume, the PCD shall generate for a time t_{RESET} a voltage less than or equal to $V_{\text{OV,RESET}}$ (rms) at the output of the pickup coil of the EMV TEST PICC. $V_{\text{OV,RESET}}$ shall be measured as described in Table 3.7. Refer to Annex A.2 for the value of $V_{\text{OV,RESET}}$ (on previous slide). Refer to Annex A.5 for the value of t_{RESET} .

from Annex A.5 (Table A.6)

Parameter	PCD Value		PICC Value		Units
	Min	Max	Min	Max	
t_{RESET}	5.1	10	0	5	ms

Modulated PCD Measurements

- The ISO/IEC 14443 standard defines two possible modulation types, Type A and Type B.
- For communication from PCD to PICC, both Type A and Type B use Amplitude Shift Keying (ASK).
- The amplitude of the carrier is switched between V_1 and V_2 , creating a lower level when the field is at value V_2 .
- The requirements of the lower level as well as of the envelope of the carrier for the two modulation types of ISO/IEC 14443 are defined in Section 3.3 of EMV document.
- Type A communication from PCD to PICC uses the modulation principle of ASK 100%. The carrier is turned on and off, creating a lower level when turned off. In practice, it will result in a modulation depth of 95% or higher. The lower level for Type A modulation is referred to as “pause” by ISO/IEC 14443-2. Table 3.10 describes how to measure the Type A modulation characteristics of a PCD.
- Type B communication from PCD to PICC uses the modulation principle of ASK 10%. The amplitude of the carrier is reduced to create a lower level with a modulation index m_i . The requirements on the lower level as well as on the envelope of the carrier are defined below. Table 3.12 describes how to measure the Type B modulation characteristics of a PCD.

Modulated PCD Measurements (For ISO14443A)

1. Place the EMV – TEST PICC in the Operating Volume of the PCD. Apply no modulation to J2 of the EMV – TEST PICC. Configure the EMV – TEST PICC with linear load.
2. Send a WUPA command by means of the PCD Test Environment as described in Annex B.4.
3. Capture the WUPA signal sent by the PCD at the output of the pickup coil of the EMV TEST PICC and analyze the modulation characteristics.
 - For this section, V represents the envelope of the signal measured at the output of the pickup coil of the EMV – TEST PICC, placed in the Operating Volume of the PCD. V_1 is the initial value measured immediately before any modulation is applied by the PCD. V_2 , V_3 and V_4 are defined as follows:
 - $V_2 = 0.05V_1$
 - $V_3 = 0.6V_1$
 - $V_4 = 0.9V_1$
 - The falling edge is that part of the envelope V , where V decreases from V_4 to V_2 . The rising edge is that part of the envelope V , where V increases from V_2 to V_4 .

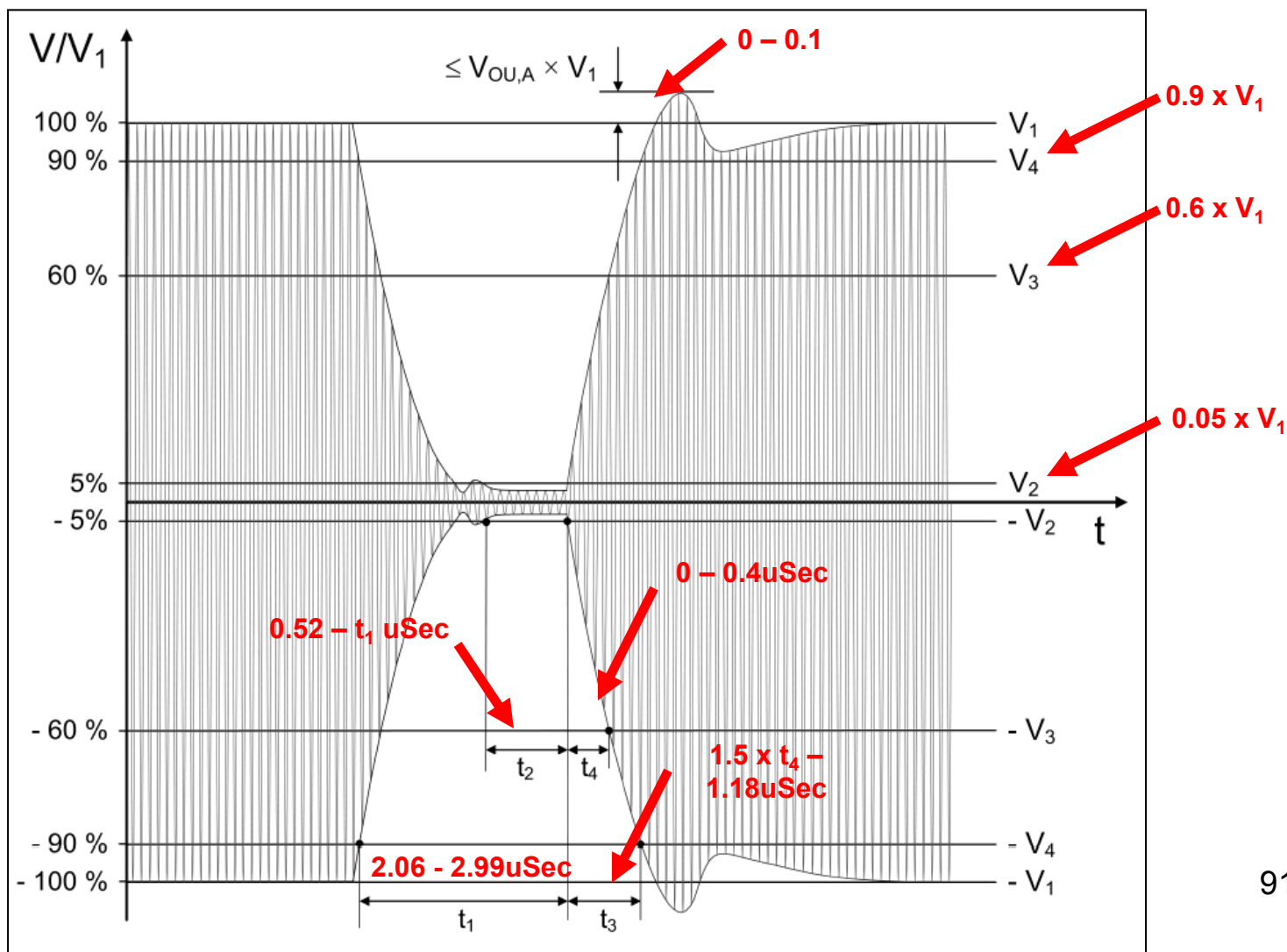
Modulated PCD Measurements (For ISO14443A)

- The PCD shall modulate the Operating Field in the Operating Volume in such a way that the signal measured at the output of the pickup coil of the EMV – TEST PICC has the following characteristics (see also Figure 3.1):
- The time between V_4 of the falling edge and V_2 of the rising edge shall be t_1 .
- If V does not decrease monotonically from V_4 to V_2 , the time between a local maximum and the time of passing the same value before the local maximum shall be t_5 . This shall only apply if the local maximum is greater than V_2 .
 - Ringing following the falling edge shall remain below $V_{OU,A}V_1$.
 - V shall remain less than V_2 for a time t_2 .
 - V shall increase monotonically to V_3 in a time t_4 .
 - V shall increase monotonically to V_4 in a time t_3 .
 - Overshoots immediately following the rising edge shall remain within $(1 \pm V_{OU,A})V_1$.
- The modulation characteristics shall be measured as described in Table 3.10. Refer to Annex A.2 for the values of t_1 , t_2 , t_3 , t_4 , t_5 and $V_{OU,A}$.

Topic	Parameter	Value Min	Max	Units
Modulation PCD→PICC (Type A)	t_1	2.06	2.99	μs
	t_2	0.52	t_1	μs
	t_3	$1.5 \times t_4$	1.18	μs
	t_4	0	0.44	μs
	t_5	0	0.50	μs
	$V_{OU,A}$	0	0.1	-

Modulated PCD Measurements (For ISO14443A)

- Figure 3.1—Lower Level – Type A Waveform



Modulated PCD Measurements (For ISO14443B)

1. Place the EMV – TEST PICC in the Operating Volume of the PCD. Apply no modulation to
2. J2 of the EMV – TEST PICC. Configure the EMV – TEST PICC with linear load.
3. Send a WUPB command by means of the PCD Test Environment (Refer to Annex B.4).
4. Capture the WUPB signal sent by the PCD at the output of the pickup coil of the EMV – TEST PICC and analyze the modulation characteristics.
 - For this section, V represents the envelope of the signal measured at the output of the pickup coil of the EMV – TEST PICC, placed in the Operating Volume of the PCD. V_1 is the initial value measured immediately before any modulation is applied by the PCD. V_2 is the lower level.
 - The modulation index (m_i), V_3 and V_4 are defined as follows:

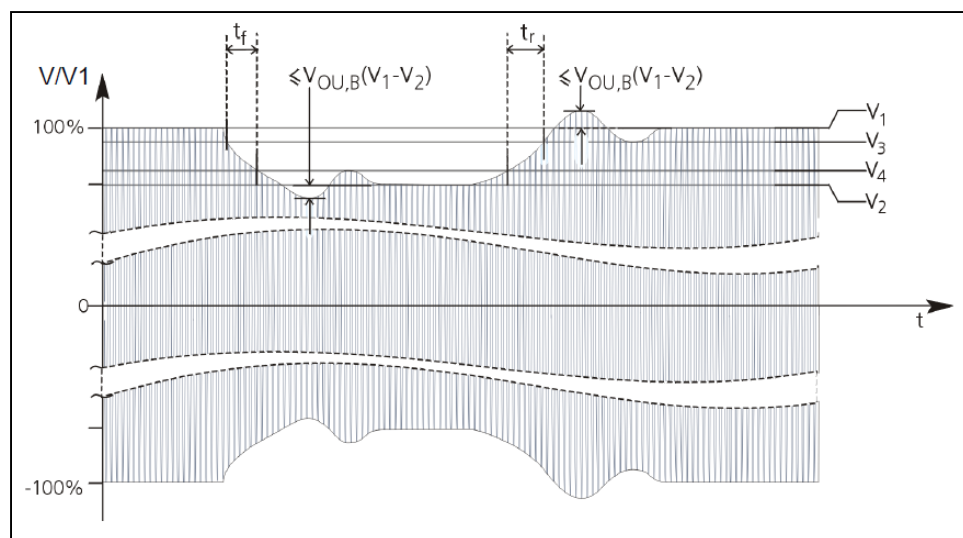
$$m_i = \frac{V_1 - V_2}{V_1 + V_2}$$

$$V_3 = V_1 - 0.1(V_1 - V_2)$$

$$V_4 = V_2 + 0.1(V_1 - V_2)$$

Modulated PCD Measurements (For ISO14443B)

- The PCD shall modulate the Operating Field in the Operating Volume in such a way that the signal measured at the output of the pickup coil of the EMV – TEST PICC has the following characteristics (see also Figure 3.2):
 - The modulation index (m_i) of the signal shall be **mod_i**.
 - V shall decrease monotonically from V_3 to V_4 (i.e. the falling edge) in a time **t_f**.
 - V shall increase monotonically from V_4 to V_3 (i.e. the rising edge) in a time **t_r**.
 - The rising and falling edges of the modulation shall be monotonic.
 - Overshoots and undershoots following the falling and rising edge shall be less than **V_{OU,B}(V₁-V₂)**.
- The modulation characteristics shall be measured as described in Table 3.12. Refer to Annex A.2 for the values of **mod_i**, **t_f**, **t_r** and **V_{OU,B}**.



Topic	Parameter	Value		Units
		Min	Max	
Modulation PCD→PICC (Type B)	mod_i	$9.0 + 0.25 z$	$15.0 - 0.25 z$	%
	t_f	0	1.18	μs
	t_r	0	1.18	μs
	V_{OU,B}	0	0.1	-

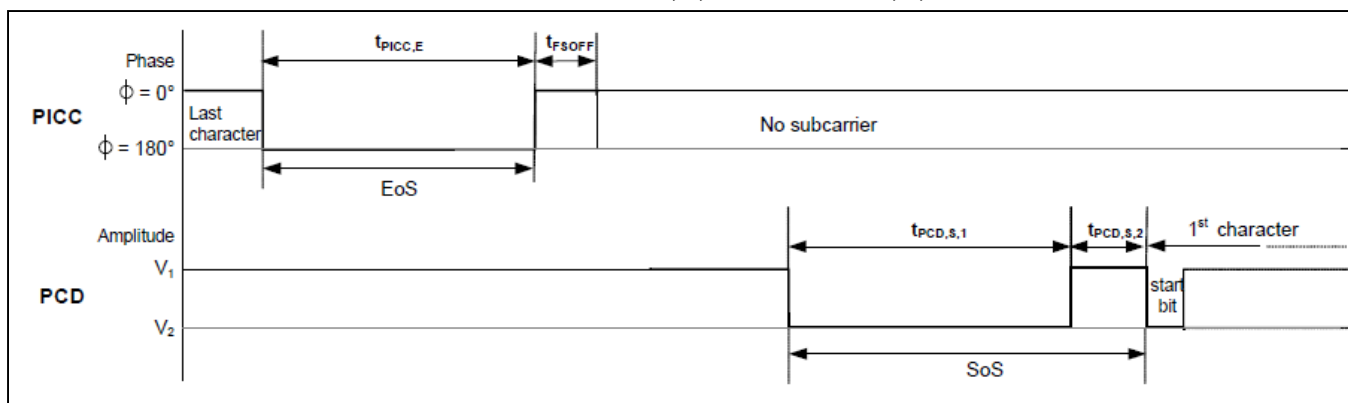
PCD Receiver Quality

(PCD Requirements for Modulation PICC to PCD)

- This section lists the requirements for the reception capabilities of a PCD to interpret the modulation applied by the PICC. Table 3.15 describes the measurement procedure that verifies whether a PCD functions properly with the EMV – TEST PICC that applies modulation characteristics at the border of the tolerance interval.
- 1. Calibrate EMV TEST - PICC
- 2. Place the EMV – TEST PICC in the Operating Volume of the PCD in a position with $0 \leq z \leq 2\text{cm}$.
- 3. Request the PCD to send a valid command to the EMV – TEST PICC by means of the PCD Test Environment as described in Annex B.4. Return a correct response by means of the EMV– TEST PICC and verify if the PCD functions properly. Perform the measurement for Type A and Type B.
- 4. Place the EMV – TEST PICC in position ($r=0$, $\phi =0$, $z=2$, $\theta =0$) of the Operating Volume of the EMV – TEST PCD. Configure the EMV – TEST PICC with non linear load.
- 5. Connect a square wave generator to J2 of the EMV – TEST PICC with a frequency of 847 kHz ($f_c/16$). Regulate in such a way that the square wave modulates the carrier with amplitude $V_{s2,pp}$ (peak to peak) measured at J2 of the EMV – TEST PCD with the EMV – TEST CMR. Refer to Annex A.3 for the value of $V_{s2,pp}$.
- 6. Place the EMV – TEST PICC in the Operating Volume of the PCD in a position with $2 < z < 4$ cm.
- 7. Request the PCD to send a valid command to the EMV – TEST PICC by means of the PCD Test Environment as described in Annex B.4. Return a correct response by means of the EMV – TEST PICC and verify if the PCD functions properly. Perform the measurement for Type A and Type B.

Synchronization Testing (ISO14443B only)

- Type A does not have a synchronization sequence. For PCD to PICC communication Type A uses 100% ASK. The lower level is a sufficient trigger to start the demodulation and to indicate the start of the first symbol.
- For ISO14443B, the PCD shall code Start of Sequence as follows:
 - $t_{PCD,S,1}$ with carrier low (modulation applied), followed by $t_{PCD,S,2}$ with carrier high (no modulation applied)
- Refer to Annex A.4 for the values of $t_{PCD,S,1}$ and $t_{PCD,S,2}$.



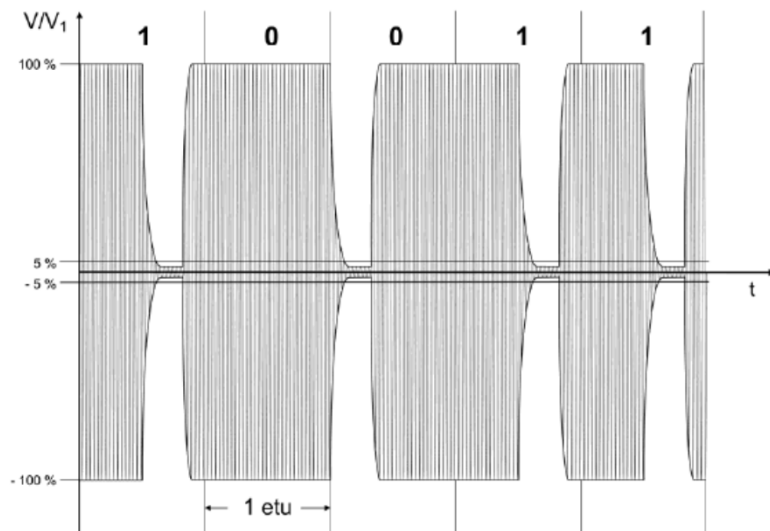
Topic	Parameter	PCD Value		PICC Value		Units
		Min	Max	Min	Max	
Type B	$t_{PCD,S,1}$	1280	1408	1264	1424	$1/f_c$
	$t_{PCD,S,2}$	256	384	240	400	$1/f_c$

Synchronization Testing (ISO14443B only)

- For establishing a phase reference $\emptyset 0$, the PCD shall proceed as follows:
 - After any command from the PCD, the PCD shall ignore any subcarrier generated by the PICC during a time **TR0_{MIN}**.
 - The subcarrier as detected during TR1 shall be taken as phase reference $\emptyset 0$.
 - *If after **TR1_{MAX}** no phase transition is detected, then the PCD may resort to exception processing (transmission error). If a phase transition is detected before **TR1_{MIN}**, then the PCD may resort to exception processing (transmission error).*
- If after the synchronization time TR1, the PCD detects:
 - a subcarrier phase transition $\emptyset 0$ to $\emptyset 0 + 180^\circ$
 - followed by a subcarrier with phase $\emptyset 0 + 180^\circ$ for **t_{PICC,S,1}**
 - followed by a subcarrier phase transition $\emptyset 0 + 180^\circ$ to $\emptyset 0$
 - followed by the subcarrier with phase $\emptyset 0$ for **t_{PICC,S,2}**
 then the PCD shall decode this as SoS.

Bit Coding (Type A & B)

- Bit coding used for Type A is Modified Miller with ASK 100% modulation depth.
- Bit coding used for Type B is NRZ-L coding with ASK 10%



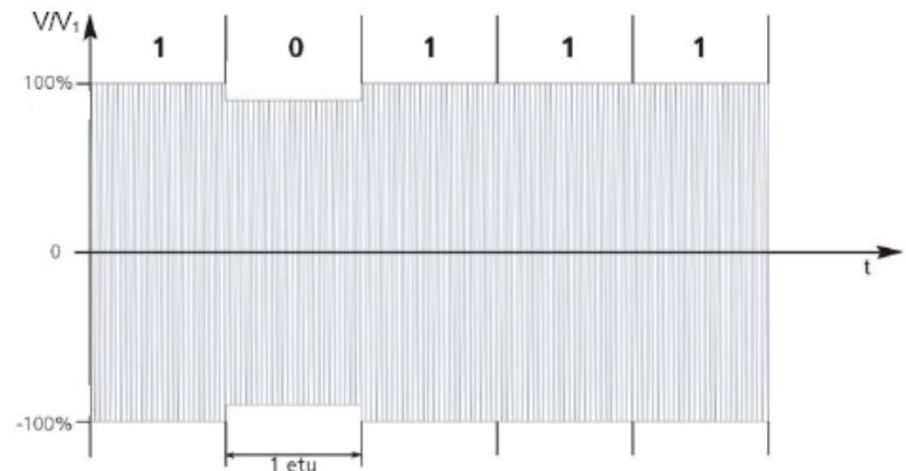
ASK 100% for Type A

The following symbols are defined:

Symbol X: After half the bit duration a lower level occurs.

Symbol Y: For the full bit duration no modulation occurs.

Symbol Z: At the beginning of the bit duration a lower level occurs.



ASK 10% for Type B

The following symbols are defined:

Symbol L: The carrier is low (modulation applied) for the full bit duration.

Symbol H: The carrier is high (no modulation applied) for the full bit duration.

Symbol Synchronization

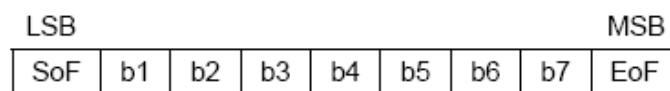
- Type A does not require synchronization before symbols.
- For Type B the separation between one character and the next is defined as the Extra Guard Time (EGT).
- The time between 2 consecutive characters sent by the PCD to the PICC shall be **EGT_{PCD}**.
- Refer to Annex A.4 for the value of **EGT_{PCD}**.

De-Synchronization

- De-synchronization is based on a violation of the regular encoding/decoding rules for a Logic “0” and a Logic “1”.
 - For Type A
 - EoS PCD → PICC
 - PCD shall code EoS as Symbol Y
 - EoS PICC → PCD
 - PCD shall decode EoS as Symbol F. (The carrier is not modulated with the subcarrier for one bit duration.)
 - For Type B
 - EoS PCD → PICC
 - a time $t_{PCD,E}$ with carrier low (modulation applied), followed by a transition to carrier high
 - EoS PICC → PCD
 - If PCD detects the following it shall decode as EoS
 - » a subcarrier phase transition $\emptyset 0$ to $\emptyset 0 + 180^\circ$
 - » followed by the subcarrier with phase $\emptyset 0 + 180^\circ$ for a time $t_{PICC,E}$
 - » followed by a subcarrier phase transition $\emptyset 0 + 180^\circ$ to \emptyset

Frame Size (Type A)

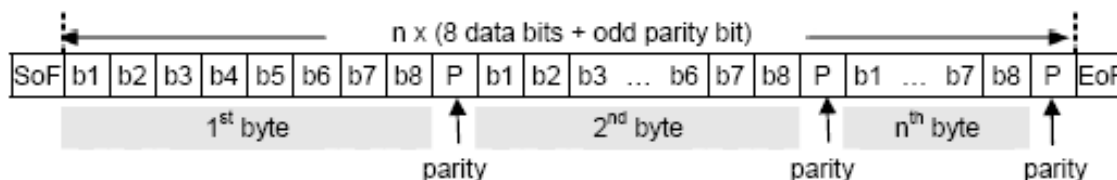
- Type A uses Short Frame (SOF, 7 bits of data, EOF) and Standard Frame (SOF, 8 data bits + odd parity bit (with $n \geq 1$), EOF)



Type A Short Frame

- Type A PCD → PICC:

- SOF = Logic 0
- EOF = Logic 0



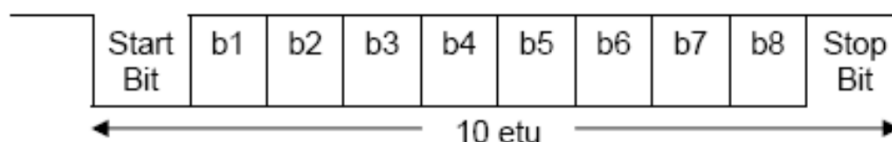
Type A Standard Frame

- Type A PICC → PCD:

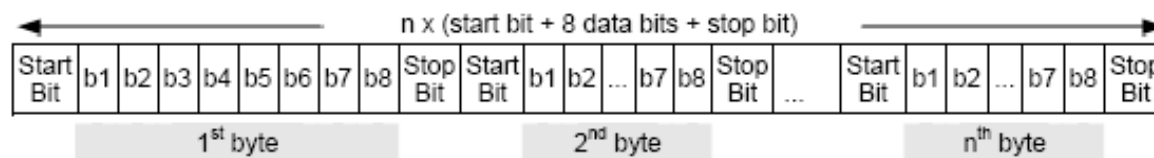
- SOF = Logic 1
- EOF = Each 8 data bits in a standard frame shall be followed by an odd parity bit. The parity bit P shall be set such that the number of 1s is odd in (b1 to b8, P).

Frame Sizes (Type B)

- Type B defines the character and frame format with the communication using LSBit first data format. Each 8 data bits are transmitted with a Logic “0” start bit and a Logic “1” stop bit.
- The frame format uses the characters separated by stop and start bits, as Type B does not utilize SOF or EOF.



Type B Character Format



Type B Frame Format

Command Frame Timing

- This section specifies the requirements for the different Frame Delay Times for Type A and Type B. The Frame Delay Time (FDT) is defined as the time between two sequences transmitted in opposite directions.
- What is measured on the reader (PCD) side is:
 - Frame Delay Time PCD → PICC (for Type A and B)

FDT_A	Minimum	Maximum
$FDT_{A,PCD}$	$FDT_{PCD,MIN}$	n.a.
$FDT_{A,PICC}$	$FDT_{A,PICC}$ with $n = 9$ (see Table 4.2)	<ul style="list-style-type: none"> $FDT_{A,PICC}$ with $n = 9$ for WUPA, REQA, ANTICOLLISION, and SELECT $FWT_{ACTIVATION}$ for RATS FWT for all other commands

Type A Timings Summary
Table

FDT_B	Minimum	Maximum
$FDT_{B,PCD}$	$FDT_{PCD,MIN}$	n.a.
$FDT_{B,PICC}$	$TR0_{MIN} + TR1_{MIN}$	<ul style="list-style-type: none"> FWT_{ATQB} for ATQB FWT for all other commands

Type B Timings Summary
Table

- Where $FDT_{A,PCD}$, $FDT_{B,PCD}$, etc. are defined in the specification and the ISO 14443 Standard.

Type A Command Set

- Type A Command Set

PCD Command	PICC Response
WUPA	ATQA
REQA	ATQA
ANTICOLLISION CL1	UID CL1
ANTICOLLISION CL2	UID CL2
ANTICOLLISION CL3	UID CL3
SELECT CL1	SAK
SELECT CL2	SAK
SELECT CL3	SAK
HLTA	—
RATS	ATS

Type B Command Set

- Type B Command Set

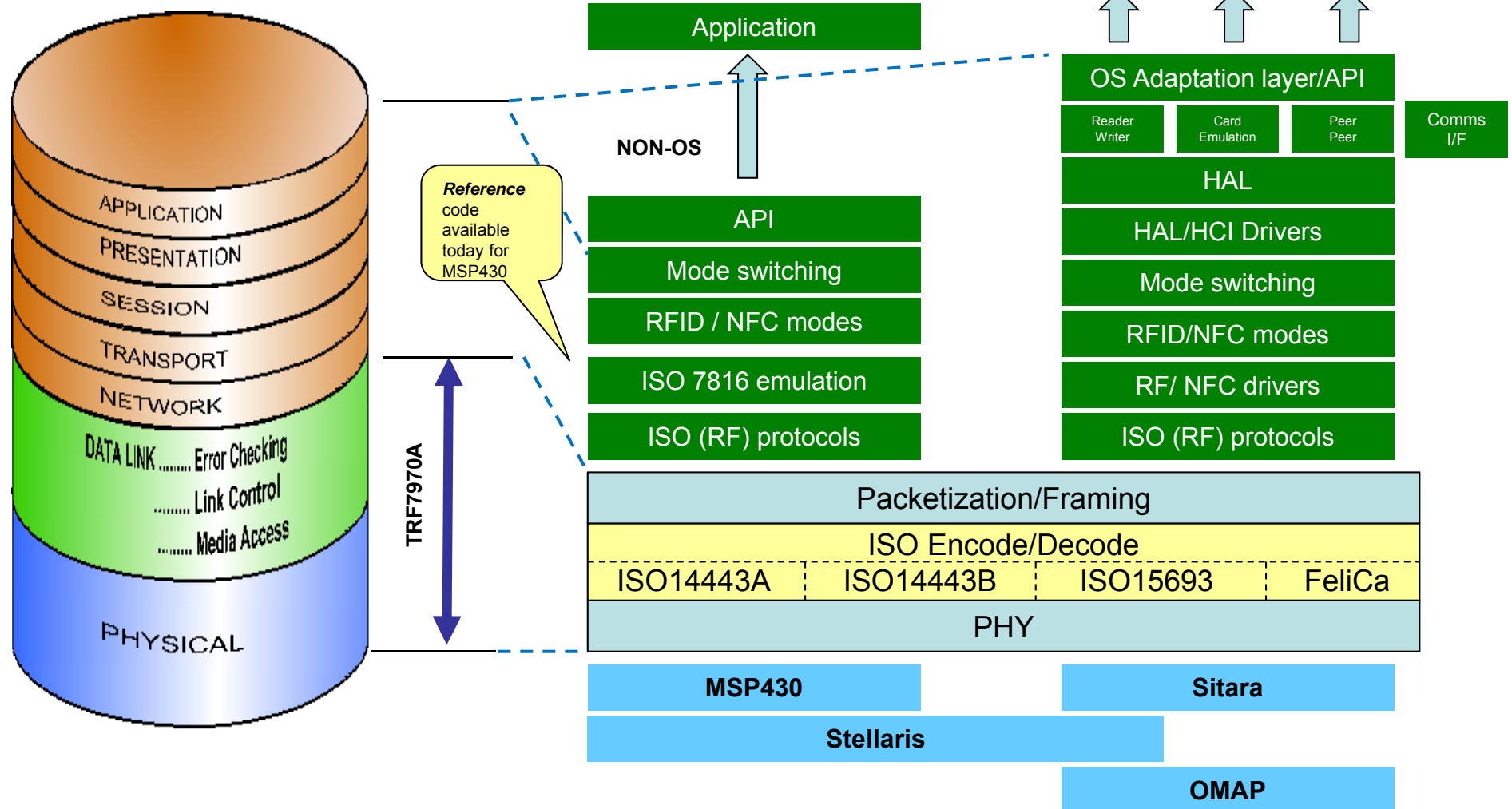
PCD Command	PICC Response
WUPB	ATQB
REQB	ATQB
ATTRIB	Answer to ATTRIB
HLTB	'00'

Break

Using TRF796x/6xA/70A with MCU

- **TRF Firmware Overview**
 - **Protocol/Mode Specific Details**
 - **RFID Operations**
 - **NFC Operations**
 - **Card Emulation**
 - **Peer to Peer**

TRF79xx NFC/RFID FW Overview

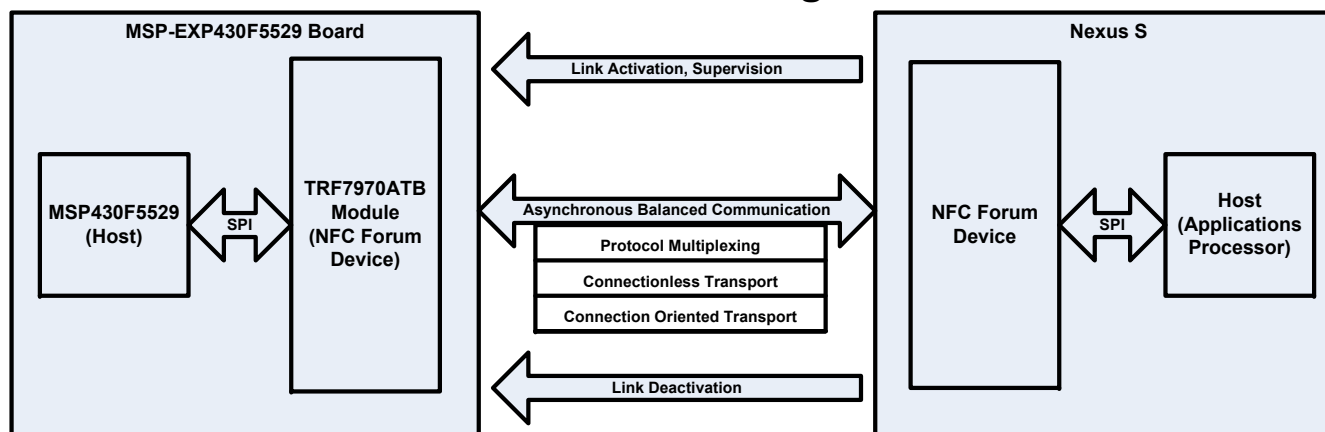


Firmware Use Case for NFC

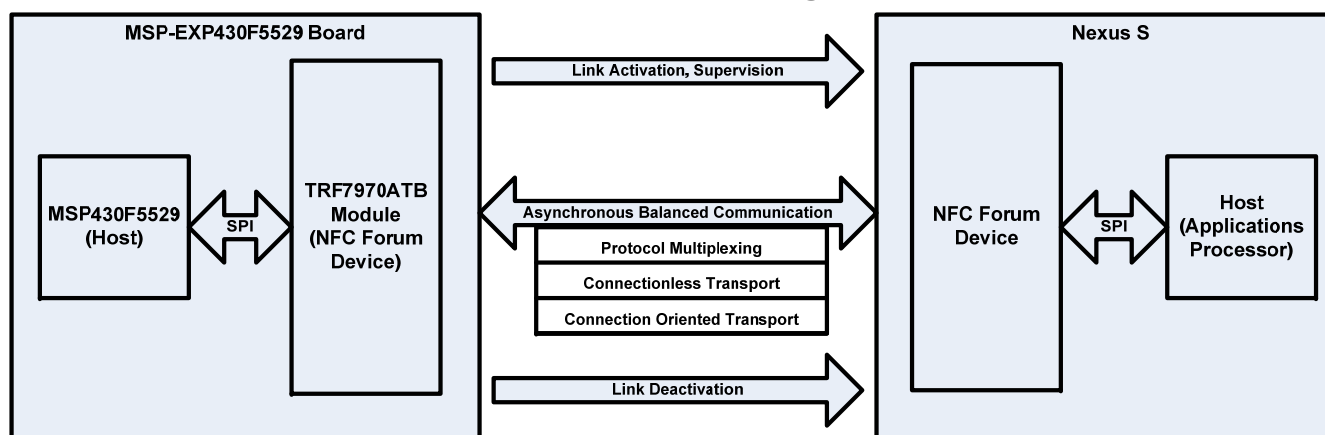
- **Peer to Peer** – this is used for bi-directional communication between two systems.
- Example use cases
 - Bootstrap Loading a Firmware update over NFC Link (between two MCUs)
 - WiFi configuration (CC3000 example)
 - Passing text, URI, file transfer, etc.

P2P Firmware Flow Diagrams

- Reference Model for NFC Peer to Peer using LLCP with Nexus S as Initiator

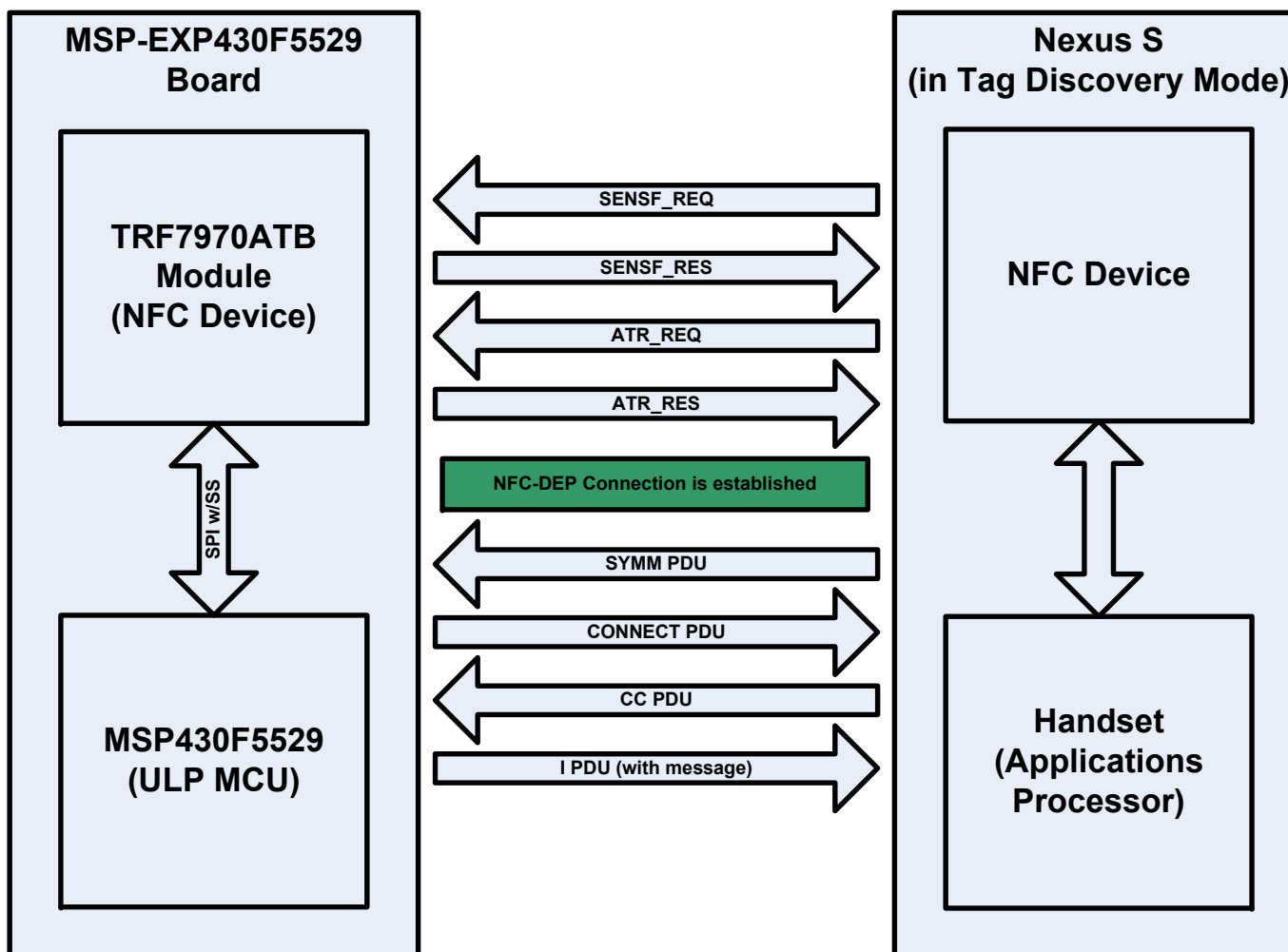


- Reference Model for NFC Peer to Peer using LLCP with TRF7970A as Initiator



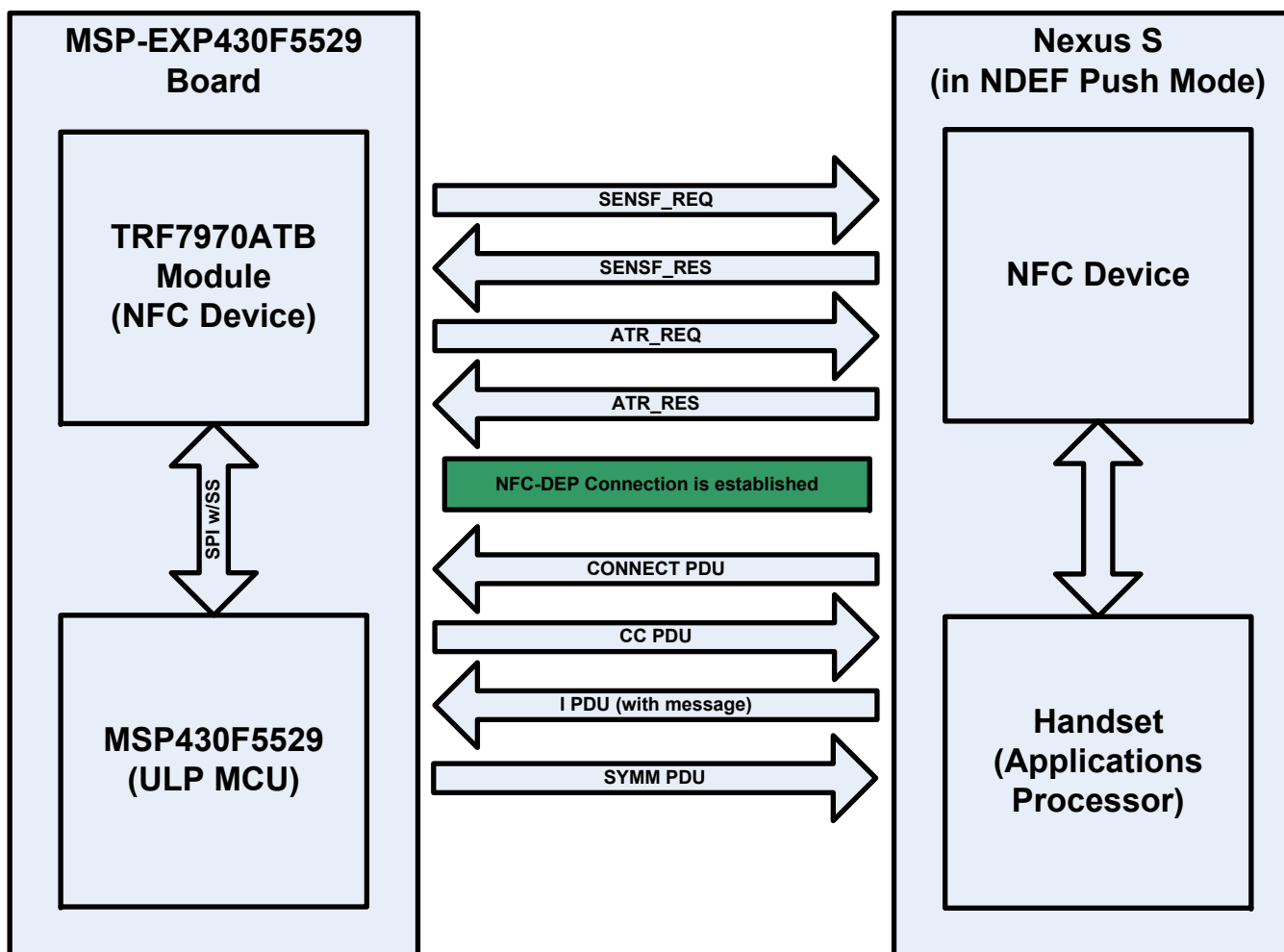
P2P Command Flow Diagram #1

Command Request/Response Exchange Flow When Nexus S is Initiator
(according to NFC Specifications)



P2P Command Flow Diagram #2

Command Request/Response Exchange Flow When TRF7970A is Initiator
(according to NFC Specifications)



Configuration of the TRF7970A for P2P Operations Example

- Initialize SPI w/SS by using Direct Command 0x03 → 0x83 (Software Initialization) See Table 5-18 of TRF7970A DS and NFC_Target_InitLoop() in nfc.c firmware file.
- Idle TRF7970A by using 0x00 → 0x80 (Idle) See Table 5-18 of TRF7970A DS and NFC_Target_InitLoop() in nfc.c firmware file.
- Write Registers to Configure TRF7970A for desired mode (Passive NFC Target in this example)
- Registers and values to write (in order):

Register	Value	Notes
0x09	0x21	SYS_CLK & MOD
0x01	0x23	NFC Passive Target @ 424kbps
0x0B	0x01	Regulator, could be set to 0x87 (Auto)
0x0A	0x1C	RX Special Settings for NFC Target
0x18	0x06	NFC Target Detection Level
0x17	0x01FExxxxxxxx	Example NFCID (0x01FE needed for indicating support of the NFC-DEP request, <u>xxxxxxxx</u> can be any other hex values desired)
0x16	0x01	NFC Low Field Detection Level
0x14	0x0F	FIFO IRQ Level (RX high = 96 bytes, TX low 32 bytes)
0x00	0x21	Chip Status Control

- Reset the FIFO with Direct Command 0x0F → 0x8F
- Disable/Enable RX'ers with Direct Commands 0x16, 0x17 → 0x96, 0x97, respectively
- TRF7970A is now set up as a passive NFC Target with a NFCID of 0x01FExxxxxxxx, waiting for field to be presented and commands issued.

Interaction with Android Handset

- As previously explained, when using NFC on Android handset with TRF7970A, it can be observed that polling is taking place. Case Statements are used in the MSP430 code to handle these IRQs whereby when the field changes and generates the IRQ, the IRQ is serviced and then register 0x19 status is read. For this effort, the value of 0x93 being returned in Register 0x19 is the starting point or trigger, and these are the details behind starting the NFC P2P operations, after TRF7970A is configured.
- The value of 0x93**16** (1001001**12**) being returned in Register 0x19 indicates that the first command (from the handset) was FeliCa or ISO14443A type @ 424kbps. (see TRF7970A Data Sheet for full register definition) The FIFO Status Register (0x1C) is then read and value returned indicates there are 6 bytes waiting in the TRF7970A FIFO. These bytes are then retrieved from the FIFO and this is the NFC Command known as SENSEF_REQ (for further information, please see Section 6.4 and on in the NFC-F Technology Portion of the NFCForum-TS-DigitalProtocol-1.0 document).
- An app note and source code package is being generated on this topic and all the relevant details (packets with byte definitions, etc.) will be included.

DEMO P2P

Firmware Use Case for NFC

- **Card Emulation** – this is used when “tag” needs to be programmed in system, by an MCU
- Example use cases
 - Bluetooth or BLE Connection and Pairing
 - Payment/Ticketing
 - Access Control

Background

- The NFC Forum and the Bluetooth Special Interest Group (SIG) recently collaborated to produce application document entitled, *Bluetooth Secure Simple Pairing using NFC*.
 - NFCForum-AD-BTSSP_1.0, http://www.nfc-forum.org/resources/AppDocs/NFCForum_AD_BTSSP_1_0.pdf
- This collaborative document is a follow on to a previously released specification by the NFC Forum entitled, NFC Forum Connection Handover Specification, which began to define the structure and sequence of interactions that enable two NFC-enabled devices to establish a connection using other wireless communication technologies. Connection Handover combines the simple, one-touch set-up of NFC with high-speed communication technologies, such as WiFi or Bluetooth.
- The purpose or intent of this presentation is to explain how a developer/integrator using the Texas Instruments NFC Transceiver (TRF7970A) would actually begin to implement the NFCForum-AD-BTSSP_1.0 specification in their embedded application.

Note: The presentation is intended to serve as a friendly interpretation/simplification guide to the embedded application development process for engineers who may not necessarily have the time become RFID/NFC document experts, too. This presentation is not intended to be a primer on NFC or Bluetooth, as the intended audience might already be very familiar with basic concepts, intended use cases, acronyms, etc. of NFC and Bluetooth.

Agenda

- Reference Documents Overview
- Selection, Connection and Starting Application Options Overview
- Handover to a Bluetooth Carrier Overview
- Configuration of the TRF7970A as NFC Tag Type 4 (ISO14443B)
- Configuration of the TRF7970A as NFC-A, NFC-B or NFC-F target
- Formation of the binary content on the NFC Forum Tag or Target, based on application specific requirements
 1. Tag Formats for a Single Bluetooth Alternative Carrier (SBAC)
 - with BT MAC Address only
 - with BT MAC Address and optional 'OOB' data
 2. Tag Format for "Static" Handover with pre-programmed Handover Select Message (which does not include Simple Pairing Hash C and Randomizer R values)
 3. Tag/Target Format for a Negotiated Handover (for devices that require dynamic mutual authentication, using Simple Pairing Hash C and Randomizer R values)
 - Note: The NFC Forum/BT SIG Document presents this case as Peer to Peer (P2P) operation only, however this can probably be done in either Card Emulation or P2P mode, especially in cases where programmable MCU is present and operating both the TRF7970A and the BT radio)
- Interacting with mobile NFC and Bluetooth Enabled Device (i.e. handset) with the embedded MCU connected to NFC and Bluetooth hardware examples.

Reference Documents

- Documents used during implementing the examples and during the creation of this presentation were:
 - TRF7970A Data Sheet (SLOS743)
 - ISO/IEC14443-3, -4
 - ISO/IEC7816-4
 - Type 4 Tag Operation Specification
 - NFCForum-TS-Type-4-Tag_2.0
 - NFC Data Exchange Format (NDEF) Specification
 - NFCForum-TS-NDEF_1.0
 - NFC Digital Protocol Technical Specification
 - NFCForum-TS-DigitalProtocol-1.0
 - NFC Forum Connection Handover Technical Specification
 - NFCForum-TS-ConnectionHandover_1_2
 - *Bluetooth* Secure Simple Pairing Using NFC
 - NFCForum-AD-BTSSP_1.0

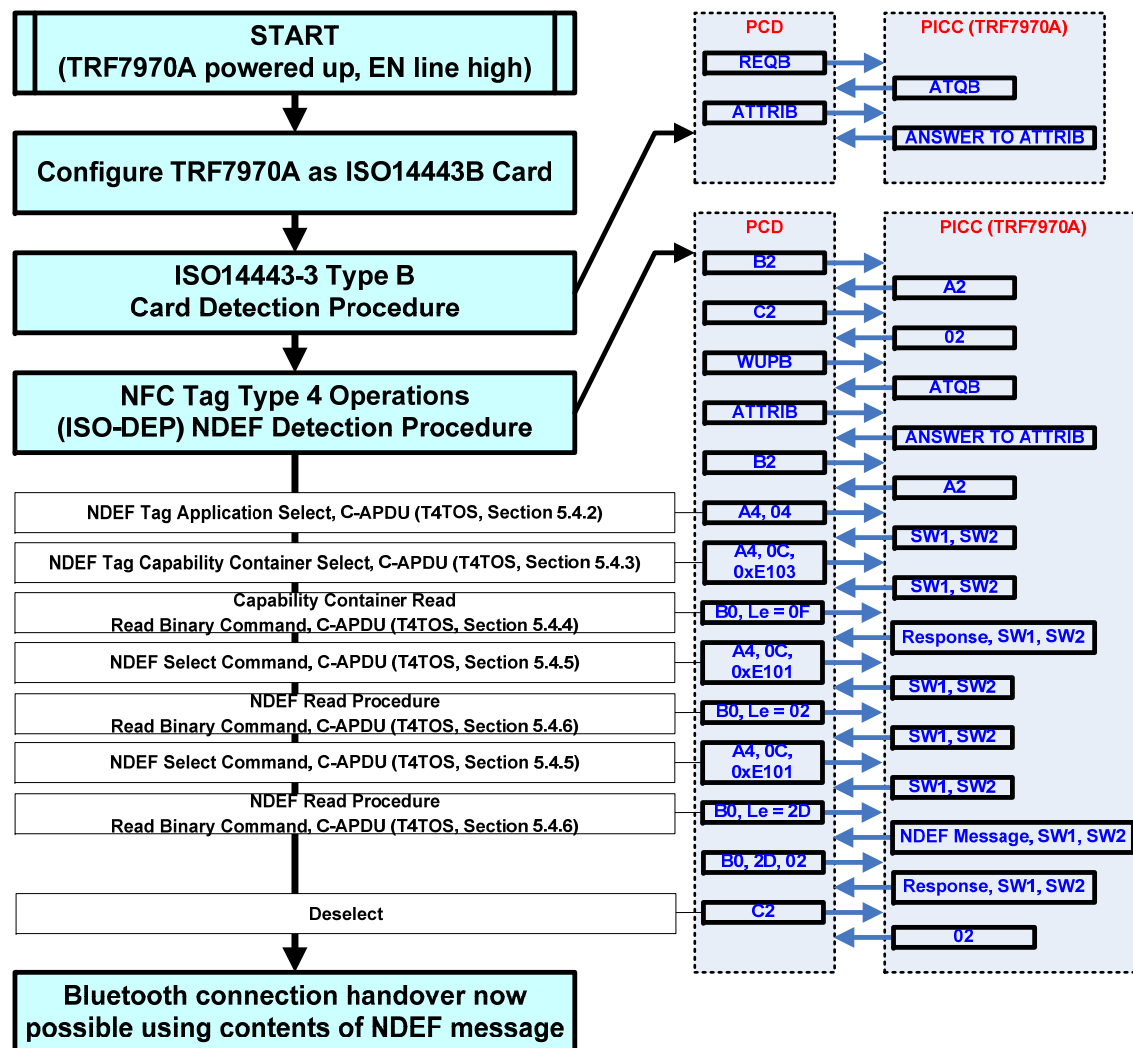
Selection, Connection and Starting Applications Options Overview

- The use of the NFC technology can enhance the user experience of applications that use the *Bluetooth* technology. The enhancements can be any of the following areas:
 - Select a *Bluetooth* device
 - Discovering a *Bluetooth*-enabled device typically uses the Inquiry procedure to discover other *Bluetooth* devices in the vicinity of the discovering device. NFC can simplify the discovery process by eliminating the Inquiry process by providing the *Bluetooth* address and other optional parameters related to a specific *Bluetooth*-enabled device. This removes the need for the user to select the appropriate device from a (potentially long) list. **The result is a more seamless wireless user experience.**
 - Securely connect to a *Bluetooth* device
 - NFC can simplify the process of authenticated pairing between two *Bluetooth* devices by exchanging authentication information over an NFC link. Devices that comply with [BLUETOOTH_CORE] and subsequent versions use Secure Simple Pairing (SSP). SSP provides a stronger level of security, yet makes it easier for the user to perform pairing. SSP explicitly introduces the notion of Out-of-Band (OOB) pairing. The information (Hash C and Randomizer R, described in Section 3.3) can be exchanged over an NFC link to be used as part of the OOB pairing process.
 - Start an application on a *Bluetooth* device
 - NFC can be used to start an application to provide good user experience. For example, the user touches their NFC Forum device to another NFC Forum device to exchange contact information. Starting an application upon NFC 'touch' action is implementation specific. In some cases, the 'touch' could even allow the user to select the application to execute.

Handover to a Bluetooth Carrier Overview

- The *Bluetooth* SIG defined a mechanism called “Secure Simple Pairing” ([BLUETOOTH_CORE], Volume 2, Part H, Section 7) to simplify the process of pairing two *Bluetooth* devices. Secure Simple Pairing defines four different association models, one of them using an Out-of-Band channel such as NFC.
- The NFC Forum Connection Handover Technical specification defines the mechanism and format of the messages to exchange Alternative Carrier information between NFC Forum Devices or between an NFC Forum Tag and NFC Forum Device. Specifically, *Bluetooth* OOB data can be exchanged in Connection Handover Request and/or Select messages as Alternative Carrier information.
- The *Bluetooth* SIG has defined a Media-type per [RFC2046] for ‘Secure Simple Pairing OOB’ communication, and “[application/vnd.bluetooth.ep.oob](#)” should be used as the [NDEF] record type name. The payload for this type of record is then defined by the Extended Inquiry Response (EIR) format specified in the *Bluetooth* Core Specification ([BLUETOOTH_CORE], Volume 3, Part C, Section 8).

Using the TRF7970A in Card Emulation for SSP Overview



Configuration detail of the TRF7970A as NFC Tag Type 4 (ISO14443B)

- Initialize SPI w/SS by using Direct Command 0x03 → 0x83 (Software Initialization)
See Table 5-18 of TRF7970A DS
- Idle TRF7970A by using 0x00 → 0x80 (Idle) See Table 5-18 of TRF7970A DS
- Write Registers to Configure TRF7970A for desired mode (ISO14443B in this example)
- Registers and values to write (in order):
 - 0x09 → 0x01 (this sets bit 7 to 0 (for 13.56MHz crystal operation)
 - 0x01 → 0x25 (sets bit 5 for NFC/Card Emulation and bits 0, 1, and 2 for ISO14443B operations)
 - 0x0B → 0x87 (automatic)
 - 0x0A → 0x3C (RX Special Settings for ISO14443B)
 - 0x18 → 0x07 (NFC Target Detection Level set)
 - 0x17 → write continuous with NFCID/PUPI (i.e. 0x80, 0x12, 0x34, 0x56)
 - 0x16 → 0x03 (NFC Low Field Detection Level set)
 - 0x02 → 0x00 (ISO14443B TX Options, no EGT after each byte)
 - 0x00 → 0x21 (Chip Status Control Set)
- Reset the FIFO with Direct Command 0x0F → 0x8F
- Disable/Enable RX'ers with Direct Commands 0x16, 0x17 → 0x96, 0x97, respectively
- TRF7970A is now set up as an ISO14443B transponder with a NFCID/PUPI of 0x80123456₁₆, waiting for field to be presented and commands issued.

C Code for Configuring TRF7970A as NFC Tag Type 4B (ISO14443B)

//The following function is responsible for Initializing the TRF7970A device. The function takes no input parameters.

```
static int Init(ParameterList_t *TempParam)
{
    unsigned char val;
    unsigned char Data[11] = "\x80\x12\x34\x56"; //NFC ID (PUPI = 80123456)

    TRF7970Command(TRF7970_SOFT_INIT_CMD); //MAKE SURE SPI IS INITIALIZED
    TRF7970Command(TRF7970_IDLE_CMD);
    TRF7970WriteRegister(TRF7970_MODULATOR_CONTROL_REG, 0x01); //NO SYS CLK OUTPUT
    TRF7970WriteRegister(TRF7970_ISO_CONTROL_REG, 0x25); //NFC Card Emulation, ISO14443B @106kbps
    TRF7970WriteRegister(TRF7970_REGULATOR_CONTROL_REG, 0x87); //Auto @ +5VDC IN
    TRF7970WriteRegister(TRF7970_RX_SPECIAL_SETTINGS_REG, 0x3C); //this value could be: 0x30, 0x34, 0x38 or 0x3C
    TRF7970WriteRegister(TRF7970_NFC_TARGET_LEVEL_REG, 0x07); // Set the Target Detection Level to Max.
    TRF7970WriteRegisterContinuous(TRF7970_NFC_ID_REG, Data, 4); // Set the NFCID to be sent.
    TRF7970WriteRegister(TRF7970_NFC_LO_FIELD_LEVEL_REG, 0x03); //MAX Value
    TRF7970WriteRegister(TRF7970_ISO14443B_OPTIONS_REG, 0x00); //no EGT, could also be 0x02
    TRF7970WriteRegister(TRF7970_CHIP_STATUS_CTRL_REG, 0x21); //full power @ +5VDC IN

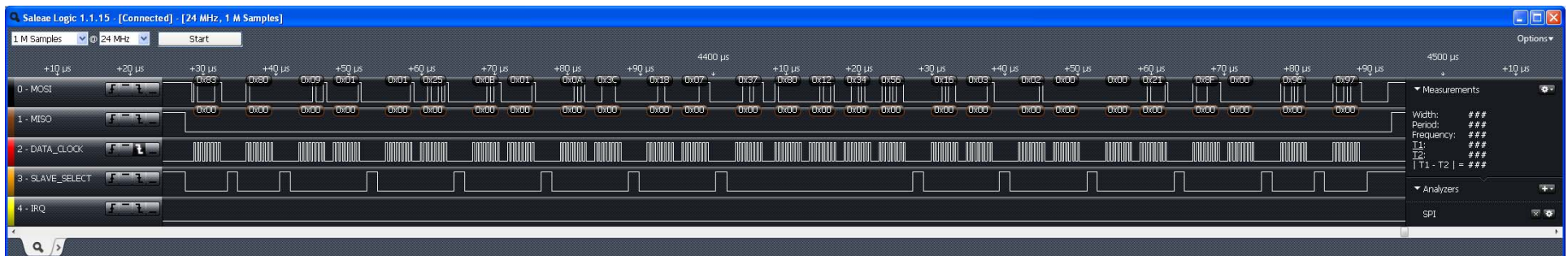
    SSITRF7970WriteDirectCommandWithDummy(TRF7970_RESET_FIFO_CMD);

    BufferIndex = 0;
    TRF7970Command(TRF7970_STOP_DECODERS_CMD);
    TRF7970Command(TRF7970_RUN_DECODERS_CMD);

    return(0);
}
```

Card Emulation Configuration (Logic Analyzer View)

- In the figure below, one can see the initialization and configuration of the TRF7970A as the C code (from previous slide) is being executed to place the TRF7970A in ISO14443B Card Emulation Mode.
- After this, the TRF7970A is waiting for HF field to be presented and REQB command to be issued.



Formation of the binary content

(Tag Format for SBAC, BT Address Only)

from Table 7: Binary Content of a Sample *Bluetooth* OOB Data on an NFC Forum Tag

Offset (Octets)	Content	Length (Octets)	Explanation
0	0xD2	1	NDEF Record Header: MB=1b, ME=1b, CF=0b, SR=1b, IL=0b, TNF=010b
1	0x20	1	Record Type Length: 32 octets
2	0x21	1	Payload Length: 33 octets
3	0x61 0x70 0x70 0x6C 0x69 0x63 0x61 0x74 0x69 0x6F 0x6E 0x2F 0x76 0x6E 0x64 0x2E 0x62 0x6C 0x75 0x65 0x74 0x6F 0x6F 0x74 0x68 0x2E 0x65 0x70 0x2E 0x6F 0x6F 0x62	32	Record Type Name: application/vnd.bluetooth.ep.oob
35	0x08 0x00	2	OOB Optional Data Length (8 octets)
37	0x06 0x05 0x04 0x03 0x02 0x01	6	Bluetooth Device Address: 01:02:03:04:05:06

Demos

THANKS!!!!!!