T E C H N I C A L   D A T A S H E E T

- NFC Forum Mandated Type 1 Tag Format

Topaz 13.56MHz Near Field Communication (NFC) / Radio Frequency Identification (RFID) Read/Write IC

ISO/IEC18092, 21481 & 14443A Compatible

Part Number: TPZ-201-series

www.innovision-group.com/topaz

INNOVISION RESEARCH & TECHNOLOGY PLC

M2000-1057-02
Revision 02 June 2007 (non-NDA)

Table of Contents

Datasheet Revision History

Revision	Date	Page(s)	Description
02	06/07		Registered logo, document number and general update for non-NDA usage, updated part number

UK Head Office

Innovision Research & Technology plc
33 Sheep Street
Cirencester
Gloucestershire
GL7 1RQ, UK

Telephone: +44 (0) 1285 888200
Fax: +44 (0) 1285 888190

Email: topaz@innovision-group.com
Web: www.innovision-group.com/topaz

1. Description

The Topaz IC, (part number IRT5011), has been developed by Innovision Research & Technology plc to address Near Field Communication (NFC) and Radio Frequency Identification (RFID) tagging applications working to the ISO/IEC 18092, ISO/IEC 21481 and ISO/IEC 14443A standards.

The Topaz IC based tag has been mandated by the NFC Forum as the Type 1 Tag Format to work with NFC devices.

The Topaz IC is a two terminal device designed to be connected to a loop antenna to produce a passive NFC/RFID tag operating in the standard unlicensed 13.56MHz frequency band.

The read/write data in the Topaz IC memory is EEPROM-based, allowing individual blocks to be locked into read only operation by contactless command. Once locked, the process is irreversible.

The Topaz IC is based on a physical EEPROM array size of 120 bytes.

Passive operation means that no battery is required because the Topaz IC gathers its operational energy from the interrogation field generated by the NFC Reader/Writer unit.

2. Features

- Topaz IC can be used in NFC Forum Tags/Smartposter/ One-touch Setup applications as well as general RFID
- Targeted for operation with NFC devices which work to ISO/IEC 18092 (NFCIP-1) and/or ISO/IEC 21481 (NFCIP-2)
- Designed to be compatible with the ISO/IEC 14443:2001 parts 2 and 3
- ISO/IEC 14443 type A modulation scheme
- Passive RFID tag operating in the unlicensed 13.56MHz band
- Read and Write (R/W) operation
- One Time Programmable (OTP) & Write Once Read Many (WORM) operation
- Typical operating range up to 10cm depending on tag/reader antenna coil sizes and orientation relative to the reader unit
- Fast data communication rate of 106 kbit/s
- UID provision in Topaz IC to enable collision detection by means of the Reader/Writer issuing a RID (Read UID) command.
- Protection for data during the write operation by the Topaz IC only responding to commands pre-pended with a matching UID. This also provides protection in the situation where there are multiple tags in the reader field
- Fast byte write speed
- Data communications are protected by 16-bit CRC integrity checking
- EEPROM based user read/write memory area organised as 12 blocks of 8-bytes
- 7-bytes of Unique Identification (UID) number for use in data authentication/anti-cloning
- 96-bytes of user read/write memory
- 6-bytes of OTP memory
- All memory areas are individually one time lockable by RF command to prevent further modification of data and to produce read only functionality

3. Benefits

- Small die size
- Mandated as Type 1 Tag Format by the NFC Forum for operation with NFC devices in Reader/Writer mode
- Initial “Request and Answer” communication cycle between the NFC reader/writer device and the Topaz IC based NFC Tag follows the ISO/IEC 18092 and ISO/IEC 14443-3 standards
- Will operate with forthcoming ISO/IEC 18092 & ISO/IEC 21481 compliant NFC devices directly and with most existing ISO/IEC 14443 reader/writers after software modification only
- Low-power requirement
- High-integrity – 16-bit CRC protection on communications protocol
- Blocks of memory can be utilised as shadow areas for anti-tear protection measures
- Memory size and capacity is scalable for custom designs
- Two bond pad die attachment
- Wire-bond, flip-chip and module die attachment methods possible
- Suitable for operation with wide variety of antenna coil size, form factor and construction
- Fast read all command (RALL)

4. Specification

Physical/Environmental

- Die size approx 0.59 x 0.59mm (including guard ring)
- Standard 150µm thickness
- L1, L2 pad passivation opening ≥ 80µm
- 2 terminal IC for conventional wire bond or flip chip attachment
- Operating temperature range: –25°C to +50°C
- Non-operational data retention (i.e. storage temperature) range: –40°C to +70°C

Memory Map

- 16-bits (2-bytes) of metal mask product identification header ROM
- 56-bits (7-bytes) of Unique Identification (UID) number
- 768-bits (96-bytes) of user read/write memory
- User Read/Write memory arranged as 12 blocks of 8-bytes
- Each 8-byte user read/write block is individually lockable by RFID command
- For systems working on 16-byte blocks, the pairs of 8-byte blocks can be written to and locked together by the reader
- 48-bits (6-bytes) of One Time Programmable (OTP) bit area
- OTP bits can be set both individually or as multiple bits together in one command

Security

- 7-byte Unique Identification (UID) number is programmed and locked during manufacture
- Further blocks can be programmed with application specific data and then locked to provide tamper-proof contents
- OTP bits can be used for non-reversible one direction counters
- CRC protection on command and data communications to retain integrity
- All blocks, and hence all logical pages, have a one-time lock capability
- The Topaz IC can use a “Digital Certificate” or “Seal” based on the unalterable and unique identification number to authenticate and provide an appropriate level of security

General

- On-chip tuning capacitance designed for nominal 13.56MHz operation
- Read range will depend on the antenna used and reader specifications
- Fast write speed <6.5mS per byte
- “Read All” command for fast read access of complete memory contents
- Data retention >5 years
- Write operations >10,000 cycles
- Available in two forms:

  Tested wafer

  Tested, bumped, ground and sawn wafer (film on frame)
- Contact Innovision for ordering information and full part number

5. C-tune

C-tune is the on-chip capacitance across the device pads L1 & L2 (expected use: to tune a coil connected across L1 & L2 to a frequency near to 13.56MHz).

C-tune has been metal-mask selected as follows:

- C-tune standard = 21.1pF nominal

6. Topaz IC Identification

The Topaz IC carries a specific “Header ROM” value, fixed in memory area HR0, to identify that the tag is capable of carrying an NDEF Message as defined by the NFC-Forum.

Qualification of the HR0 value must be used by a NFC reader/writer in order to identify and segregate between tags based on the Topaz IC and on other Innovision ICs.

The header ROM, HR0 value is assigned as follows:

- Topaz IC (TPZ-201-series), HR0 = 11_h

7. Physical Memory Map

The 120-byte EEPROM array is arranged as 15 blocks of 8-bytes each. Each block is separately lockable.

There is an additional 2-byte Header ROM, where HR0 = 11_h identifies the tag as Topaz IC for NFC NDEF data applications. HR1 is reserved for internal use and shall be ignored.

HR0	HR1
11_h	xx_h

EEPROM Memory Map										
Type	Block No.	Byte-0 **(LSB)**	Byte-1	Byte-2	Byte-3	Byte-4	Byte-5	Byte-6	Byte-7 **(MSB)**	Lockable
UID	0	UID-0	UID-1	UID-2	UID-3	UID-4	UID-5	UID-6		Locked
Data	1	Data0	Data1	Data2	Data3	Data4	Data5	Data6	Data7	Yes
Data	2	Data8	Data9	Data10	Data11	Data12	Data13	Data14	Data15	Yes
Data	3	Data16	Data17	Data18	Data19	Data20	Data21	Data22	Data23	Yes
Data	4	Data24	Data25	Data26	Data27	Data28	Data29	Data30	Data31	Yes
Data	5	Data32	Data33	Data34	Data35	Data36	Data37	Data38	Data39	Yes
Data	6	Data40	Data41	Data42	Data43	Data44	Data45	Data46	Data47	Yes
Data	7	Data48	Data49	Data50	Data51	Data52	Data53	Data54	Data55	Yes
Data	8	Data56	Data57	Data58	Data59	Data60	Data61	Data62	Data63	Yes
Data	9	Data64	Data65	Data66	Data67	Data68	Data69	Data70	Data71	Yes
Data	A	Data72	Data73	Data74	Data75	Data76	Data77	Data78	Data79	Yes
Data	B	Data80	Data81	Data82	Data83	Data84	Data85	Data86	Data87	Yes
Data	C	Data88	Data89	Data90	Data91	Data92	Data93	Data94	Data95	Yes
Reserved	D									
Lock/Reserved	E	LOCK-0	LOCK-1	OTP-0	OTP-1	OTP-2	OTP-3	OTP-4	OTP-5	

Reserved for internal use
User Block Lock & Status
OTP bits

Block usage	
Block 0	7 bytes of Unique ID.
Blocks 1 – C	All 96 data bytes are available to the user as Read/Write memory.
Block D	Reserved for internal use.
Block E	Used for OTP (One Time Programmable) bits. The least significant 2-bytes are used to store the individual block-lock status. The most significant 6-bytes are used for the 48 OTP bits.

Figure 1: Memory Map

The Topaz IC tag includes two bytes of fixed header ROM called HR0 & HR1 as shown in figure 1 above.

Their contents are automatically included in the response packet to the RID (Read ID) and RALL (Read All) commands.

HR0 Upper nibble = 0001 should determine that it is a Topaz tag.

HR0 Lower nibble = 0001 should determine the TPZ-201-series part with 96 byte memory map,

HR1 = xx_h is undefined and should be ignored.

8. Block Diagram

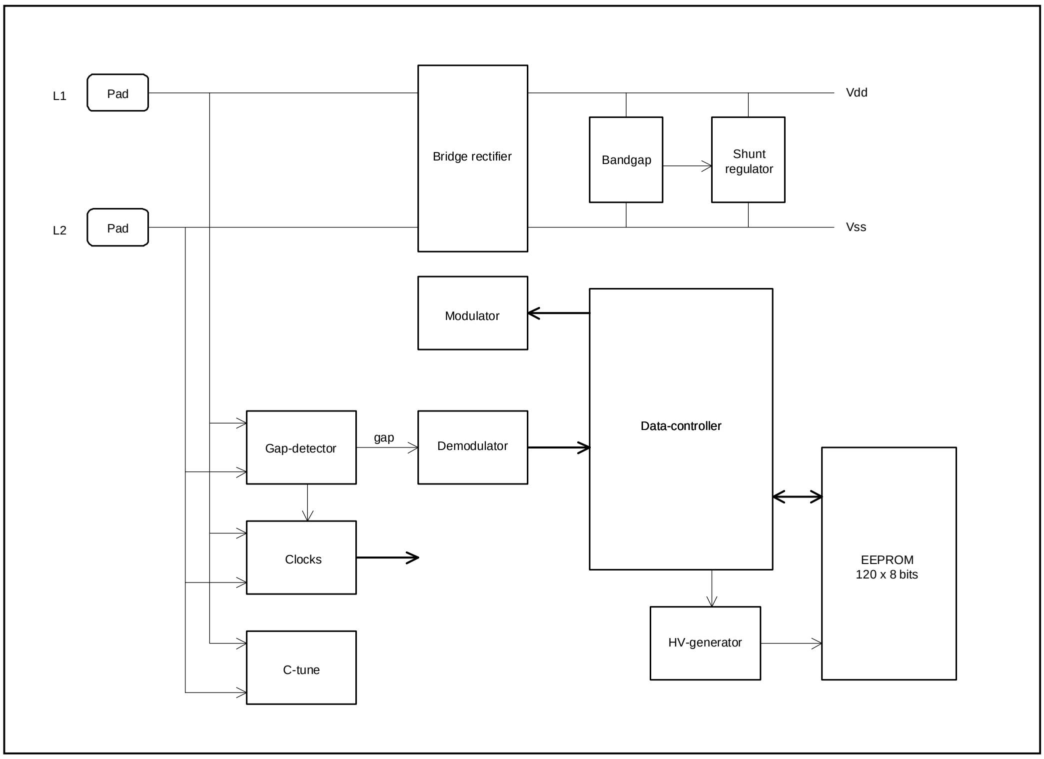


Figure 2: Outline Block Diagram

9. Device Operation

The RF interface of the Topaz IC is compliant with the type A variant in the ISO/IEC 14443-2:2001(E) standard.

- The ISO/IEC 14443 terminology uses the term PCD for Proximity Coupling Device and PICC for Proximity Integrated Circuit(s) Card. This datasheet uses the terms NFC Device in Reader/Writer mode for a PCD and the outlined Topaz IC based tag acting as a PICC.

The Topaz IC operates in accordance with ISO/IEC 14443A using the Proprietary branch at ‘Check ATQA’ (ISO/IEC 14443-3:2001(E) section 6.4.1).

A means of collision detection is provided so that the NFC Device in Reader/Writer mode knows if there is more than one tag in its field. This collision detection makes use of the 4 least significant bytes of the UID (Unique Identification number).

On power-up, the Topaz IC performs a power-on reset and remains ‘silent’ in IDLE state until a REQA or WUPA command is received, upon which it moves to READY state.

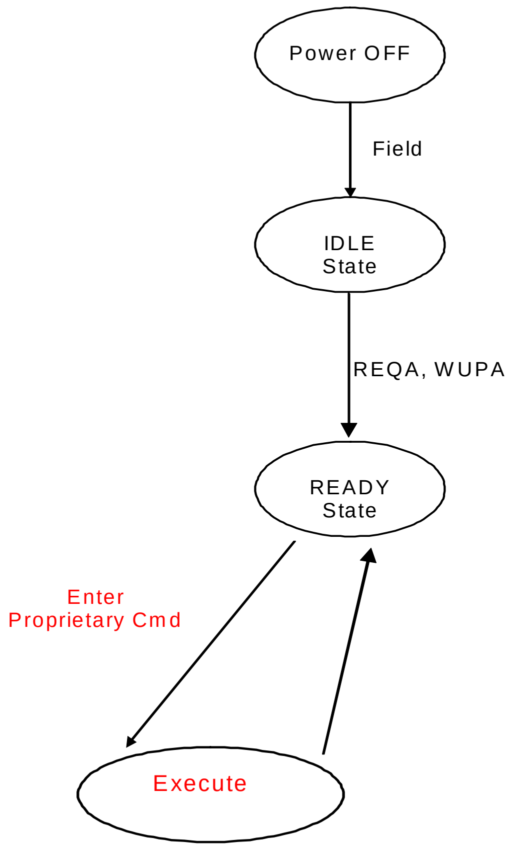


Figure 3: State Diagram

10. Commands and Data TO the Topaz IC Tag

Data communication or “signalling” to the Topaz IC tag is by means of 100% carrier modulation according to the type A variant in the ISO/IEC 14443-2:2001(E) & ISO/IEC 14443-3:2001(E) specifications.

11. Status and Data FROM the Topaz IC Tag

Data communication from the Topaz IC tag is achieved by modulation caused by varying the impedance of the tag as ‘seen’ by the coil of the NFC Device operating in Reader/Writer mode, according to the type A variant in the ISO/IEC 14443-2:2001(E) & ISO/IEC 14443-3:2001(E) specifications.

12. Frame Formats and Transmission Handling

12.1 Communication TO the tag

The communication from the NFC Device in Reader/Writer Mode to the Topaz IC tag shall consist of a short frame containing the command byte followed by a series of zero or more, proprietary frames.

Each seven or eight bit data set shall be sent to the Topaz IC tag in a separate frame, therefore a command sequence will usually consist of several frames.

S = start of frame

E = end of frame

After power-up the Topaz IC tag will only recognise the ‘S’ as a valid ‘start of command sequence’ and a command will only be considered valid if there are 7-bits between ‘S’ and ‘E’.

Command (7-bits)
“Short Frame” as specified in ISO/IEC 14443-3 type A

	lsb						msb	
S	b1	b2	b3	b4	b5	b6	b7	E

Transmitted first

Operand or Data (8-bits)
Innovision Proprietary Frame
(8-bit version of the ISO/IEC 14443-3 type A)

	lsb							msb	
S	b1	b2	b3	b4	b5	b6	b7	b8	E

Transmitted first

Figure 4: Frame Formats TO the Tag

12.2 Communication FROM the tag

Data output from the tag is sent as a single contiguous frame as shown in figure 5.

The 8-bits of each data byte (together with each byte’s parity bit) are concatenated into this single frame.

The overall frame format is the “Standard Frame” as specified for the type A variant in the ISO/IEC 14443-3:2001(E) standard [3].

S = ‘start of frame’ followed by one or more bytes (with least significant bit first in each byte).

Each byte is followed by a P (parity bit) where the number of 1’s is odd in (b1 to b8, P).

E = ‘end of frame’ (after last byte’s parity bit).

	1st Byte								2nd Byte			nth Byte			
S	b1	b2	b3	b4	b5	b6	b7	b8	P	b1 …… b8	P	b1 …… b8	P	E

Figure 5: Frame Format FROM the Tag

12.3 Transmission Handling

The transmission between an NFC Device and the Topaz IC tag is half duplex and operates on the ‘NFC Device talks first’, command-response basis.

REQA & WUPA commands sent to a Topaz IC tag will generate a two byte ATQA response according to the ISO/IEC 14443-3:2001(E) standard.

All other commands generate a response comprised of more than two bytes as shown in Table 1 below.

Table 1: Command-Response Byte Count

Command	Command bytes	Response bytes
REQA	1	2
WUPA	1	2
RID	9	8
RALL	9	124
READ	9	4
WRITE-E	9	4
WRITE-NE	9	4

Table 2 shows details of the sequence of Command and Response bytes for the Topaz IC based tag.

With the exception of the REQA, WUPA & ATQA, a two byte CRC shall be appended to the end of all commands and responses as shown.

Table 2: Command-Response Summary

Command-Response Summary Table																		
Greyed-out frames are dummy frames – their data content shall be 00h																		
Command									Response									
REQA									ATQA0	ATQA1								
WUPA									ATQA0	ATQA1								
RID	00h	00h	00h	00h	00h	00h	CRC1	CRC2	HR0	HR1	UID0	UID1	UID2	UID3	CRC1	CRC2		
RALL	00h	00h	UID0	UID1	UID2	UID3	CRC1	CRC2	HR0	HR1	UID0	UID1	….	….	….	Block-E Byte-7	CRC1	CRC2
READ	ADD	00h	UID0	UID1	UID2	UID3	CRC1	CRC2	ADD	DAT	CRC1	CRC2						
WRITE-E	ADD	DAT	UID0	UID1	UID2	UID3	CRC1	CRC2	ADD	DAT	CRC1	CRC2						
WRITE-NE	ADD	DAT	UID0	UID1	UID2	UID3	CRC1	CRC2	ADD	DAT	CRC1	CRC2						

13. Commands & Timing

13.1 Command Format

Table 3: List of Commands (Static Memory Model)

Command		**Command Code (7-bits)** msb						lsb	**Comment** (all commands are independent)
		b7	b6	b5	b4	b3	b2	b1	
REQA	26_h	0	1	0	0	1	1	0	Request Command, type A
WUPA	52_h	1	0	1	0	0	1	0	Wake-up, type A
RID	78_h	1	1	1	1	0	0	0	Read ID – Use to read the metal-mask ROM and UID0-3 from block 0
RALL	00_h	0	0	0	0	0	0	0	Read All (all bytes)
READ	01_h	0	0	0	0	0	0	1	Read (a single byte)
WRITE-E	53_h	1	0	1	0	0	1	1	Write-with-erase (a single byte)
WRITE-NE	$1A_h$	0	0	1	1	0	1	0	Write-no-erase (a single byte)

13.2 Address Operand

The format of the 'ADD' address operand for the READ, WRITE-E & WRITE-NE commands shall be as shown in table 4 below.

Table 4: Format of Address Operand ADD

Address operand 'ADD' Block = select one of blocks 0_h – E_h Byte = select one of bytes 0 – 7							
msb							lsb
b8	b7	b6	b5	b4	b3	b2	b1
0_b	Block				Byte		

13.3 CRC

Except for the REQA & WUPA command, a 2-byte CRC shall be included in each part of the command and response sequence. If the CRC value received by the tag does not match the one it internally generates as data arrives, then the tag will halt the operation and move to 'READY' state waiting for the next command.

The CRC shall be the 16-bit version as specified under CRC-CCITT – for definition see ISO/IEC 14443-3:2001(E) Annex B: CRC_B.

CRC shall be calculated on all data bits including the header bytes HR0 & HR1, however, start, end, parity, (and the CRC bits themselves), are not included within the CRC calculation.

13.4 UID Echo

The NFC Device in Reader/Writer Mode shall provide a single tag selection feature by including the lower four bytes of UID as part of all the proprietary Read and Write commands. If the four lower bytes of UID do not match, then the Topaz IC based tag will halt operation and remain in 'READY' state waiting for the next valid command.

13.5 Detailed Timing

From ISO/IEC 14443-3:2001(E), the command timing of a single bit period shall nominally be defined using B = 9.4 µs as follows.

(i) Frames to the type 1 tag: S = 1B; data = 8B; E = 2B

(ii) Frame from the type 1 tag: S=1B; E = 2B; data = 9B per byte

Table 5: Timing & Description Definitions

Timing & Description Definitions		
Name	**Description**	**Specification**
RRDD	Reader-Reader Data Delay The time between the end of the last pause of a frame transmitted by the Reader/Writer and the first pause of the next frame to be transmitted by the Reader/Writer.	Minimum: ≥ 28 µs when last bit was 1 ≥ 23 µs when last bit was 0 Maximum: None
DRD	Topaz IC tag Device Response Delay (Frame Delay Time) “The time between the end of the last pause transmitted by the Reader/Writer and the first modulation edge within the start bit transmitted by the Topaz IC tag” (taken from the FDT definition in ISO/IEC 14443-3:2001(E) para 6.1.2)	FDT timing from ISO/IEC 14443-3:2001(E), section 6.1.2 where n: For REQA, WUPA, READ, RID, RALL: n=9 For WRITE_E: n=554 For WRITE_NE: n=281 With tolerance for Digital & Analogue elements of ± 6.5 clock cycles (13.56MHz).
RRD	Reader Response Delay Delay time from Topaz IC tag to Reader/Writer ie the time between the last modulation transmitted by the Topaz IC tag and the first gap transmitted by the Reader/Writer	ISO/IEC 14443-3:2001(E), section 6.1.3 1172/fc ≅ 86 µs
CE	Command End	
UID-echo	The four least significant UID bytes from block 0 (LSB first)	

Table 6: FDT Timing Calculations

Timing table			
Command	**n**	**$FDT_{bit-1} = 128n + 84$**	**$FDT_{bit-0} = 128n + 20$**
REQA, WUPA, READ, RID, RALL	9	1236/fc ≈ 91 µs	1172/fc ≈ 86 µs
WRITE-E	554	70996/fc ≈ 5236 µs	70932/fc ≈ 5231 µs
WRITE-NE	281	36052/fc ≈ 2659 µs	35988/fc ≈ 2654 µs

13.6 REQA/WUPA Command

Note: The diagrams in the following sections do not show lead-in, start and end of frame bits, etc.

CE = Command End = Ready State

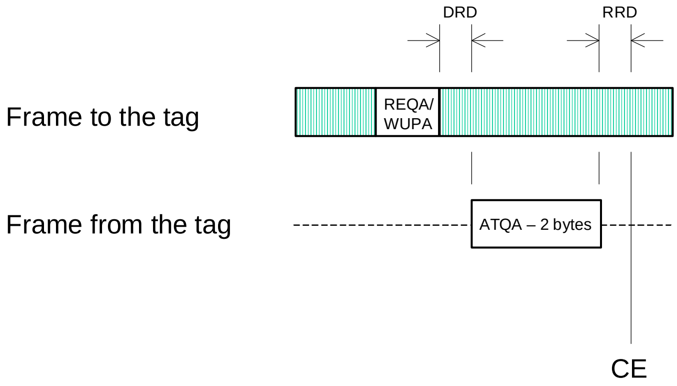


Figure 6: REQA/WUPA & ATQA Command/Response Diagram

The ATQA response bits are as follows:

Table 7: ATQA Response

msb															lsb
b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1
RFU				Proprietary Coding				UID size bit frame		RFU	Bit frame anticollision				
0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
0				C				0				0			

The ATQA = 0C00h for the Topaz IC based tag shall indicate that Innovision proprietary commands and frames are required.

None of bits b1-5 are set to '1' which shall indicate that no bit frame anticollision shall be used, as referenced in section 6.4.2.1 of ISO/IEC 14443-3:2001(E).

13.7 Read Identification (RID)

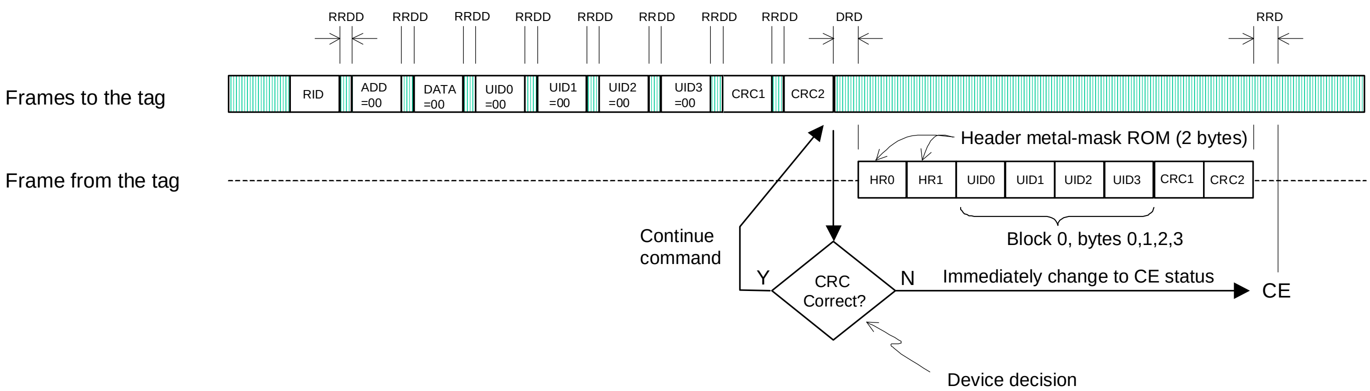


Figure 7: RID Command/Response Diagram

The RID (Read Identification) command, reads the metal-mask header bytes and the four least significant UID bytes from Block-0.

The Command frame, then Address frame, Data-byte frame, UID-echo frames & CRC frames shall be sent by the NFC Device in Reader/Writer Mode to the tag. However, the Address, Data & UID-echo bytes shall be set to zero.

If the CRC is valid then the HR0 & HR1 bytes followed by the UID-0, UID-1, UID-2, UID-3 and the frame CRC bytes will be sent back to the NFC Device.

As a pre-condition this command requires that the tag be in the READY state and afterwards the tag remains in READY state.

13.8 Read All Blocks 0-E$_h$ (RALL)

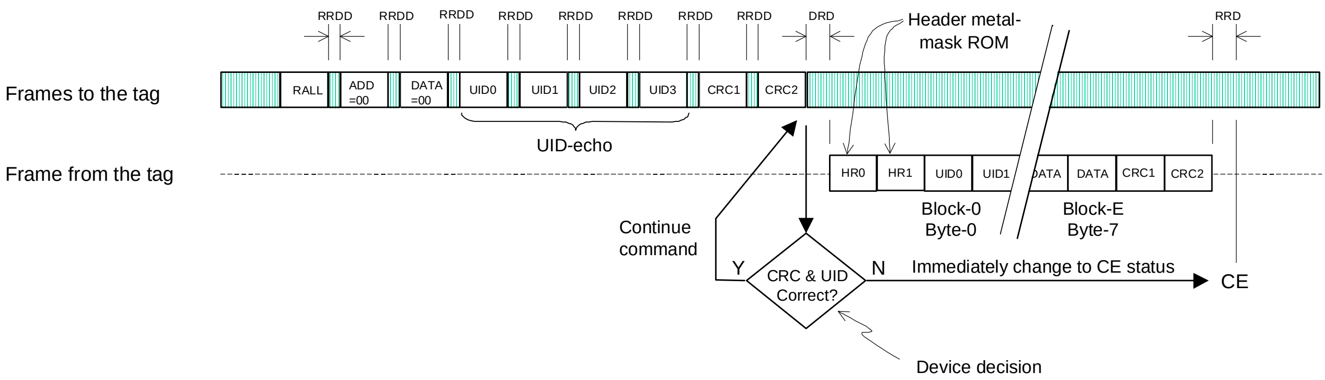


Figure 8: RALL Command/Response Diagram

The RALL command reads-out the two Header ROM bytes followed by the whole of the memory blocks 0-E$_h$.

The Command frame, then Address frame, Data-byte frame, UID-echo frames (with UID data received from previous RID command) & CRC frames shall be sent by the NFC Device in Reader/Writer Mode to the tag. However, the Address & Data-bytes shall be set to zero.

If the UID and CRC are valid the HR0 & HR1 bytes followed by the contents of memory blocks 0-E$_h$ and the frame CRC bytes will be sent back to the NFC Device.

As a pre-condition this command requires that the tag be in the READY state and afterwards the tag remains in READY state.

13.9 Read Byte (READ)

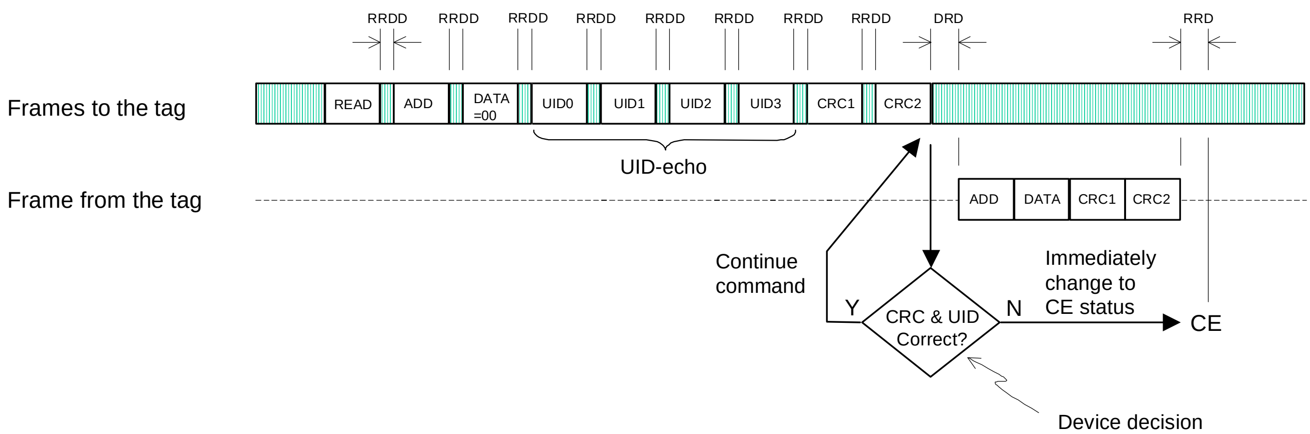


Figure 9: READ Command/Response Diagram

The READ command relates to a single EEPROM memory byte within blocks 0-E_h. The byte address, (Block number and Byte number), as defined in table 4, shall be sent with the command.

The Command frame, then Address frame, Data-byte frame, UID-echo frames (with UID data received from previous RID command) and CRC frames shall be sent by the NFC Device in Reader/Writer Mode to the tag. However, the Data-byte shall be set to zero.

If the CRC and UID are valid the requested memory data byte is read from memory. The Address, followed by the read data byte and the frame CRC bytes will be sent back to the NFC Device.

As a pre-condition this command requires that the tag be in the READY state and afterwards the tag remains in READY state.

13.10 Write-Erase Byte (WRITE-E)

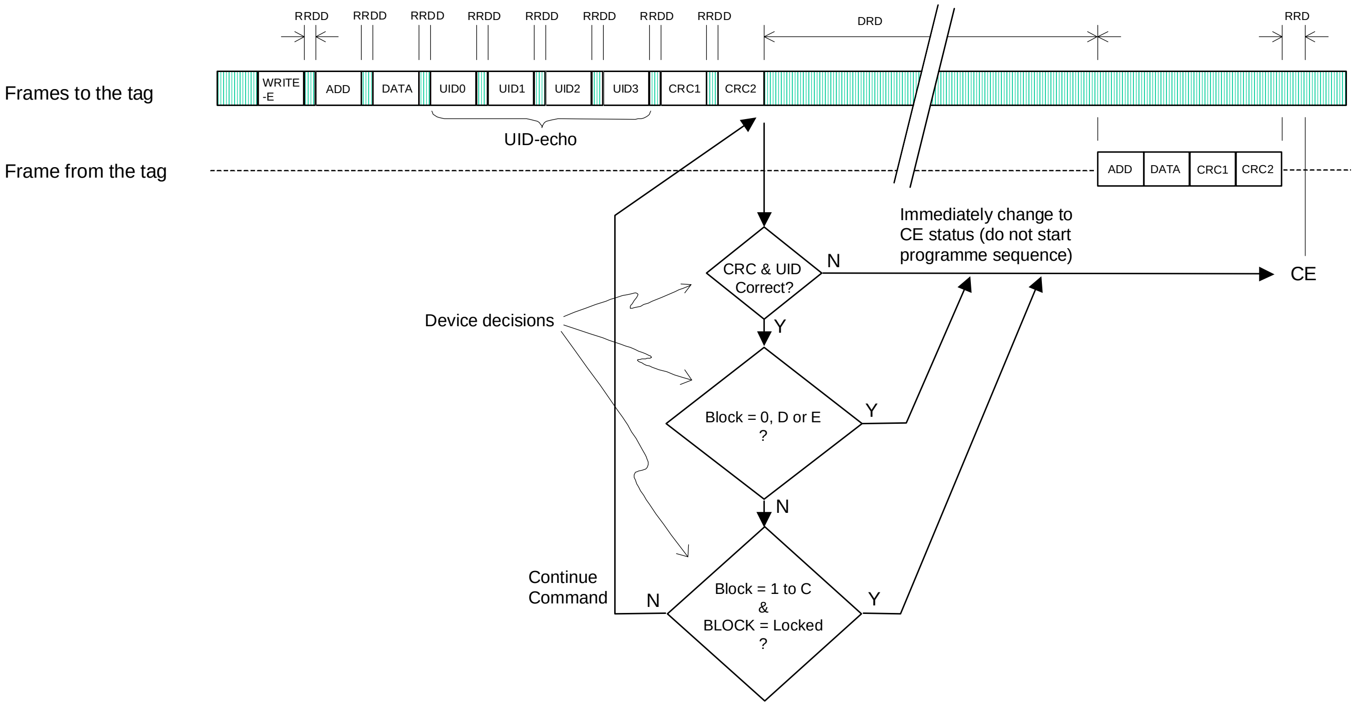


Figure 10: WRITE-E Command/Response Diagram

The WRITE-E (Write–Erase) command relates to an individual memory byte within blocks 0-E_h. The target byte address, (Block number and Byte number), as defined in table 4, shall be sent with the command. This command performs the ‘normal’ erase-write cycle, (i.e. it erases the target byte before it writes the new data).

If any of BLOCK-0 to BLOCK-D is locked then WRITE-E is barred from those blocks. Additionally, WRITE-E is always barred from Blocks 0, D or E because these are automatically in the locked condition.

The Command frame, then Address frame, Data-byte frame, UID-echo frames (with UID data received from previous RID command) and CRC frames shall be sent by the NFC Device in Reader/Writer Mode to the tag.

If the UID and CRC are valid, (and WRITE-E is not barred), the EE memory erase-write cycle is carried out. The byte is then read back from the EE memory. The address, followed by the data byte and the frame CRC bytes are then sent back to the NFC Device.

If WRITE-E is barred, the erase-write cycle is skipped – no write operation occurs – and without waiting the programme-time, the tag will enter READY status waiting for a new command.

As a pre-condition this command requires that the tag be in the READY state and afterwards the tag remains in READY state.

13.11 Write-No-Erase Byte (WRITE-NE)

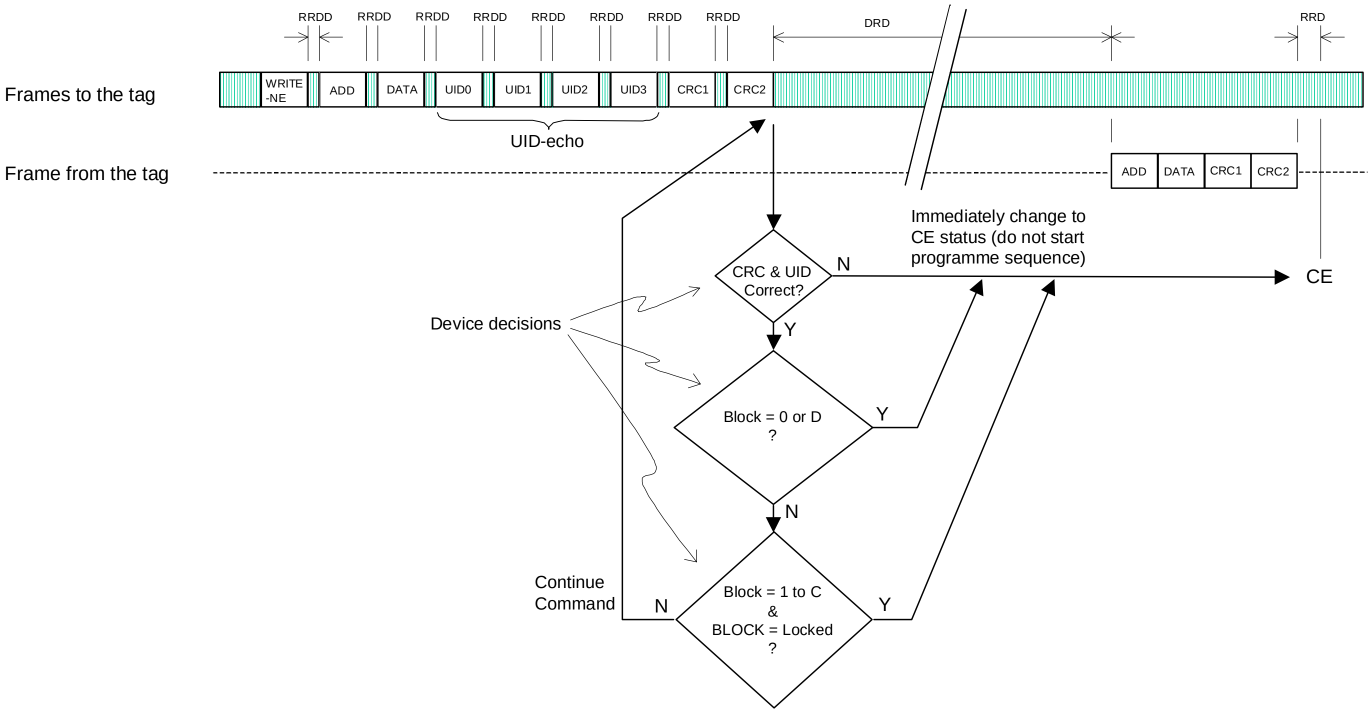


Figure 11: WRITE-NE Command/Response Diagram

The WRITE-NE (Write-no-erase) command relates to an individual memory byte within blocks 0-E_h. The target byte address, (Block number and Byte number), as defined in table 4, shall be sent with the command. This command does not erase the target byte before writing the new data, and the execution time is approximately half that of the ‘normal’ write command (WRITE-E). Bits can be set but not reset (i.e. data bits previously set to a ‘1’ cannot be reset to a ‘0’).

The WRITE-NE command is available for three main purposes:

- Lock – to set the ‘lock bit’ for a block.
- OTP – to set One-Time-Programmable bits (bytes 2 – 7 of Block-E), where between one and eight OTP bits can be set with a single WRITE-NE command.
- A fast-write in order to reduce overall time to write data to memory blocks for the first time given that the original condition of memory is zero.

If any of BLOCK-1 to BLOCK-C is locked then WRITE-E is barred from that block.

WRITE-NE is not barred from BLOCK-E to allow setting of lock and OTP bits.

The Command frame, then Address frame, Data-byte frame, UID-echo frames (with UID data received from previous RID command) and CRC frames shall be sent by the NFC Device in Reader/Writer Mode to the tag.

If the UID and CRC are valid, (and WRITE-NE is not barred), the EE memory write-no-erase cycle is carried out. The byte is then read back from the EE memory. The Address, followed by the Data byte and the frame CRC bytes are then sent back to the NFC Device.

If WRITE-NE is barred, the write-no-erase cycle is skipped – no write operation occurs – and without waiting the programme-time, the tag will return to the READY state and wait for a new command.

As a pre-condition this command requires that the tag be in the READY state and afterwards the tag remains in READY state.

14. Lock Control/Status Bits

All twelve of the memory blocks 1_h to C_h are separately lockable.

When a block's 'lock-bit' is set to a 1_b, it cannot be changed back to 0_b again and that block becomes irreversibly frozen as 'read-only'.

The lock-bits are stored in the Bytes 0 & 1 of BLOCK-E_h They operate in a bit-wise one-time-programmable fashion.

The WRITE-NE command with appropriate data pattern shall be used by the NFC Device in Reader/Writer Mode to set individual lock-bits.

A single WRITE-NE command can be used to set between one and eight lock-bits.

Table 7 shows the factory default settings.

Table 7: LOCK-0 and LOCK-1

LOCK-0 (Byte 0 of Block E_h)								LOCK-1 (Byte 1 of Block E_h)							
b7	b6	b5	b4	b3	b2	b1	b0	b7	b6	B5	b4	b3	b2	b1	b0
0_b = BLOCK-7 Unlocked	0_b = BLOCK-6 Unlocked	0_b = BLOCK-5 Unlocked	0_b = BLOCK-4 Unlocked	0_b = BLOCK-3 Unlocked	0_b = BLOCK-2 Unlocked	0_b = BLOCK-1 Unlocked	1_b = BLOCK-0 Locked	Not used	1_b = BLOCK-E Locked	1_b = BLOCK-D Locked	0_b = BLOCK-C Unlocked	0_b = BLOCK-B Unlocked	0_b = BLOCK-A Unlocked	0_b = BLOCK-9 Unlocked	0_b = BLOCK-8 Unlocked

15. UID Format

The seven byte Unique IDentification, (UID), number is locked into block 0.

See figure 1.

The byte-7 is reserved for future use and should be ignored.

The byte-6, (UID-6) is the manufacturer's identification = 25_h

16. Annex 1 – Hints & Tips

16.1 Purpose

This section is intended to clarify the communication protocol and CRC calculation.

The following is an important clarification of the Topaz IC command set.

IMPORTANT
• **Commands sent to a Topaz IC tag, (apart from the REQA or WUPA), all consist of seven bytes followed by a two byte checksum.** • **Each byte is sent within its own frame.** • **A frame start-of-message sequence proceeds each byte and a frame end-of-message sequence follows each byte.**

16.2 REQA Response

The Topaz ATQA response to a REQA or WUPA command consists of byte 0x00 followed by byte 0x0C.

Some RFID documentation specifies the REQA response as a 16-bit value, where the least significant byte is transmitted before the most significant byte. For example, the 16-bit representation of the Topaz ATQA response in this format is 0x0C00 (where 0x00 is transmitted first and 0x0C second).

16.3 Communication Example

The table below illustrates reading and writing to a Topaz tag with UID = 00,00,00,00,00,00,00,00 and all memory initialised to zero. HR1=48 for this example.

Note that bytes are transmitted with the least significant bit first. For example the table below shows that REQA (0x26, binary 010 0110) is transmitted as logic 0, logic 1, logic 1, logic 0, logic 0, logic 1 and finally logic 0.

Topaz Communication Examples (UID = 00,00,00,00)

In each column, the left-most byte (bit) is transmitted first and the right-most byte (bit) transmitted last. S refers to frame start and E to frame End sequences. The bit sequences are shown in brackets and include the odd parity bit.

Description	Command to tag (Hex)	Response from tag (Hex)
REQA	26 (S 0110010 E)	00,0C (S 00000000 1 00110000 1 E)
RID	78,00,00,00,00,00,00,D0,43 (S 0001111 E S 00000000 E …)	11,48,00,00,00,00,16,2A
RALL	00,00,00,00,00,00,00,70,8C	11,48,<120 zero bytes>,C5,2D (total 124 bytes)
READ	01,08,00,00,00,00,00,FD,32	08,00,87,C1
WRITE_E	53,08,12,00,00,00,00,41,D5	08,12,14,F2
READ	01,08,00,00,00,00,00,FD,32	08,12,14,F2
RALL	00,00,00,00,00,00,00,70,8C	11,48,00,00,00,00,00,00,00,00,12,<111 zero bytes>,62,07 (total 124 bytes)

16.4 Communication Summary

Commands sent to Topaz tag have the following format:

- First byte is 7 bits
- Remaining bytes are 8 bits
- Least significant bit is sent first
- There are no parity bits
- **A frame start sequence proceeds each byte (including the CRC bytes) and a frame end follows each byte**
- The CRC_B is appended to all commands apart from REQA and WUPA

Responses from the Topaz tag have the following format;

- All bytes are 8 bits
- Least significant bit is sent first
- A parity bit (Odd) follows each byte
- A response begins with a start frame sequence, and ends with a stop frame sequence. The response bytes (including CRC) are between these sequences.
- The CRC_B is appended to all responses apart from ATQA

16.5 CRC Clarification

The CRC is CRC_B as specified by ISO/IEC 14443-3:2001(E) Annex B.

The CRC is always calculated on 8-bit bytes.

Although the first Topaz command byte is transmitted as 7-bit, 8-bits must still be used to calculate the CRC (i.e. the 7-bits of the command must be padded with a zero in the MSB).

The CRC is calculated on all data bytes, excluding the start, end, parity and CRC bits.

The 16-bit CRC is transmitted with the least significant byte first, then the most significant byte.

16.6 Code Sample Written in C for CRC Calculation


```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>
#define CRC_A 1
#define CRC_B 2
#define BYTE unsigned char

unsigned short UpdateCrc(unsigned char ch, unsigned short *lpwCrc)
{
ch = (ch^(unsigned char)((*lpwCrc) & 0x00FF));
ch = (ch^(ch<<4));
*lpwCrc = (*lpwCrc >> 8)^((unsigned short)ch << 8)^((unsigned short)ch<<3)^((unsigned short)ch>>4);
return(*lpwCrc);
}

void ComputeCrc(int CRCType, char *Data, int Length,
BYTE *TransmitFirst, BYTE *TransmitSecond)
{
unsigned char chBlock;
unsigned short wCrc;
switch(CRCType) {
case CRC_A:
wCrc = 0x6363; /* ITU-V.41 */
```

```
break;
case CRC_B:
wCrc = 0xFFFF; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */
break;
default:
return;
}
do {
chBlock = *Data++;

UpdateCrc(chBlock, &wCrc);
} while (--Length);
if (CRCType == CRC_B)
wCrc = ~wCrc; /* ISO/IEC 13239 (formerly ISO/IEC 3309) */
*TransmitFirst = (BYTE) (wCrc & 0xFF);
*TransmitSecond = (BYTE) ((wCrc >> 8) & 0xFF);
return;
}

BYTE BuffCRC_A[10] = {0x12, 0x34};
BYTE BuffCRC_B[10] = {0x0A, 0x12, 0x34, 0x56};
unsigned short Crc;
BYTE First, Second;
FILE *OutFd;
int i;

int main(void)
{
printf("CRC-16 reference results ISO/IEC 14443-3\n");
printf("Crc-16 G(x) = x^16 + x^12 + x^5 + 1\n\n");
printf("CRC_A of [ ");
for(i=0; i<2; i++) printf("%02X ",BuffCRC_A[i]);
ComputeCrc(CRC_A, BuffCRC_A, 2, &First, &Second);
printf("] Transmitted: %02X then %02X.\n", First, Second);
printf("CRC_B of [ ");
for(i=0; i<4; i++) printf("%02X ",BuffCRC_B[i]);
ComputeCrc(CRC_B, BuffCRC_B, 4, &First, &Second);
printf("] Transmitted: %02X then %02X.\n", First, Second);
return(0);
}
```

16.7 Code Sample Written in Perl for CRC Calculation


```
#!/usr/bin/perl
# CRC calculator for Topaz
# original Aug 2003

print "Reader to tag - Enter hex for each byte, empty string to end\n";
$poly = 0x0810;          #polynomial - we xor bits 11 and 4 with in0
$crc  = 0xffff;  #initial value
$m="0"; $b=0;

for($b=0; $b<200; $b++) {
   print "byte $b: ";
   $_=<STDIN>;
   chomp;
   if ($_ eq "") {last;}
   $m = hex($_);   #data byte
   $v=0x01;       #bit marker - start at LSB of data

   for ($i=0; $i<8; $i++) {
     $crcmsb=($crc & 0x8000)>>15;            #MSB of the crc
     $din = ($m & $v)>>$i;                   #selected data bit
     $in0 = $crcmsb ^ $din;

     if ($in0) {
        $crc = $crc ^ $poly;            #xor with polynomial
     }
     $crc = ($crc << 1) & 0xffff;       #left shift the crc
     if ($in0) {$crc = $crc+1;}

     $v = $v << 1;           #next bit of data
   }
}
#printf "crc before transformation = %x\n", $crc;
```

```
#now invert and reflect

$crc = $crc ^ 0xffff;                    #invert
$out = 0;                                        #output value
for ($i=0; $i<16; $i++) {
    $j = 8*int($i/8) + (7-$i%8);         #calculate destination bit (reflection)
    $bit = ($crc>>$i) & 1;
    $out = $out + $bit*(2**$j);
}

printf "output CRC = %x\n", $out;
```

16.8 Scope Traces Illustrating Topaz Communication

This section uses oscilloscope traces to illustrate Topaz tag communication.

The traces show the following signals:

2 : Sniffer coil placed next to the reader antenna

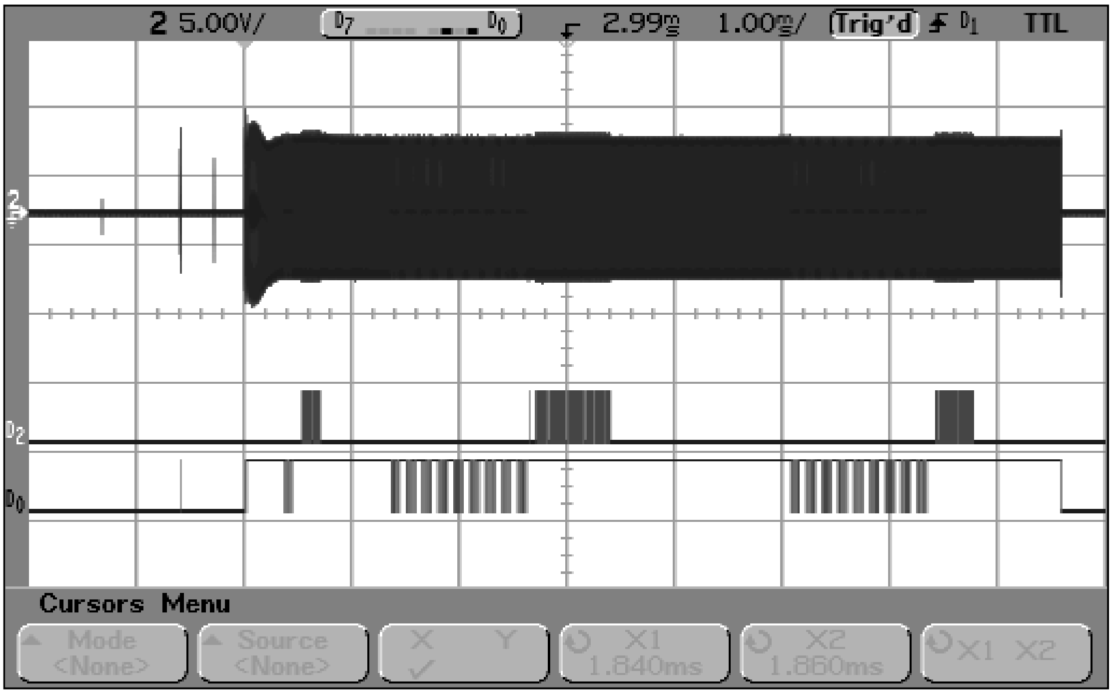
D0 : Digital signal showing transmissions from the reader to the tag

D2 : Digital signal showing transmissions from the tag to the reader

The scope traces were taken during a read of 1 byte from Topaz IC memory location 0x08, using the commands REQA, RID and READ. The UID is all zero and the data byte at 0x08 has a value of 0x00.

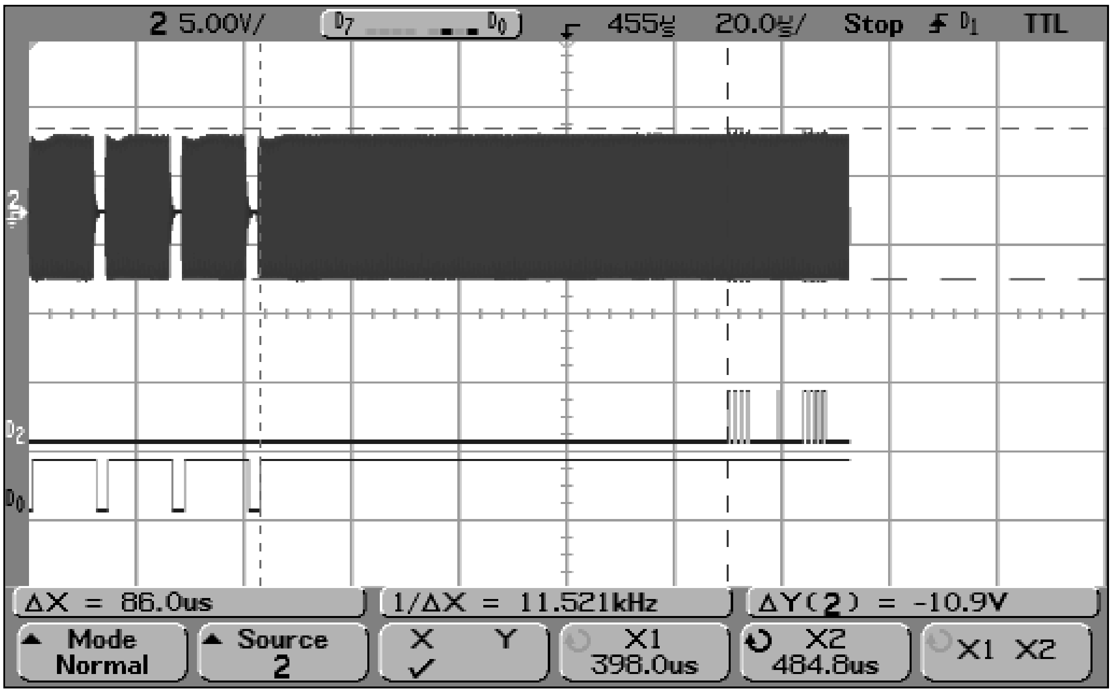
Trace 1: Entire Communication Sequence

Note that the entire communication sequence takes 7.5ms.



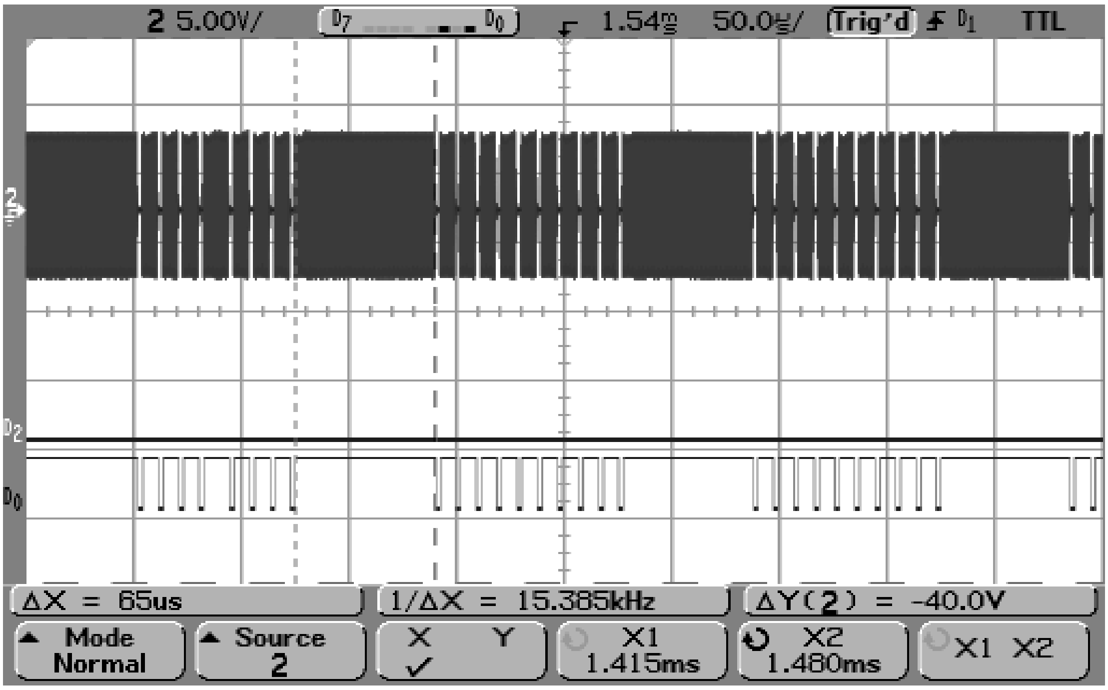
Trace 2: Delay from REQA to ATQA Response

Note that the Device Response Delay (DRD) for the REQA command is 86µs.



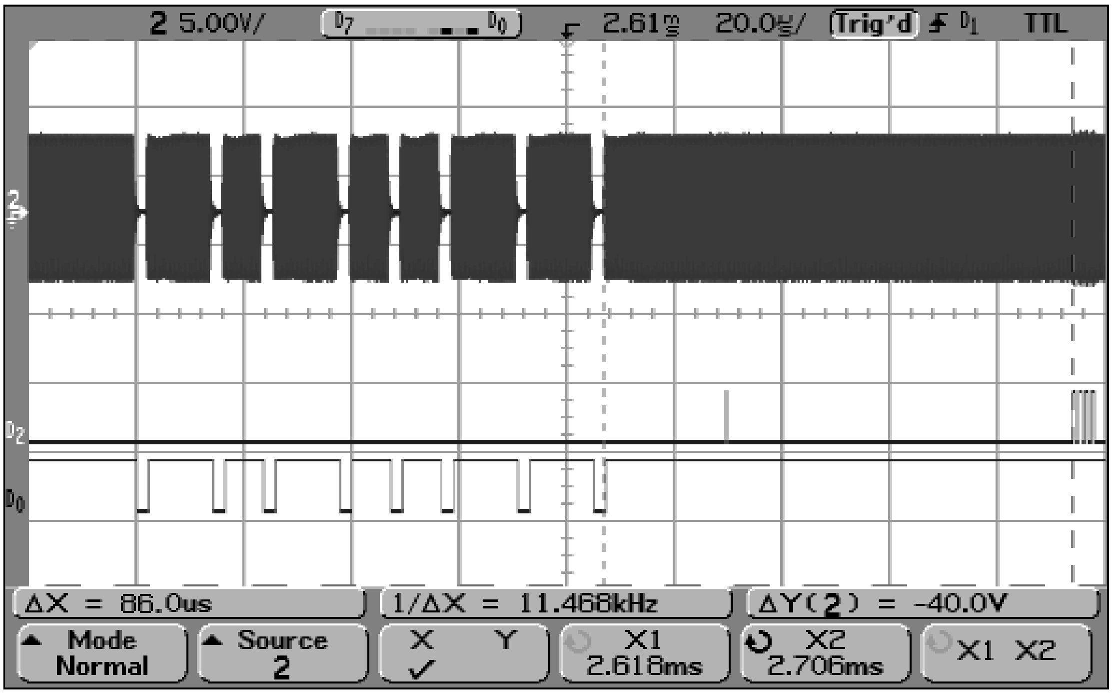
Trace 3: Start of RID Command

Note that the Reader-Reader Data Delay (RRDD) in this example is 65µs.



Trace 4: End of RID Command

Note that the Device Response Delay (DRD) for the RID command is 86µs.



Appendix A1: Terms and Conditions of Supply

1. This document is provided for internal evaluation only.

2. Innovision has endeavoured to ensure that material in the document is accurate as at the date of the document. Information, data, apparatus, products, processes, market positions, third party status or intellectual property right and materials referred to or contained in this document are dynamic and may change over time. Innovision shall not be liable for any loss (direct, indirect or consequential) associated with such change.

3. Innovision shall not be liable for improper or incorrect use of the contents of the document or of any products referred to in this document or for use of the information contained in this document for a purpose other than that for which it was provided.

4. Save in respect of death or personal injury resulting from the negligence of Innovision or Innovision's employees, agents or subcontractors negligence, Innovision expressly disclaims all express and implied warranties and conditions, so far as is legally possible.

5. Use of any information in this document to develop a product is at the risk of the party using this document.

6. Save in respect of death or personal injury resulting from Innovision or Innovision's employees and as far as legally possible, Innovision disclaims all liability for damages, costs and expenses incurred as a result of use of this document.

7. References within the document to any specific third party products, websites, processes or services or use of any trade name, product name or trade mark do not constitute or imply endorsement, recommendation by the relevant third party or favouring, endorsement or recommendation of the third party by Innovision.

8. Where information is taken from a third party source this is stated in the document and Innovision accepts no liability for the accuracy or completeness of such information.

9. Nothing in this document shall convey any licence over or transfer any intellectual property rights to or any third party.

10. Innovision's products are not authorised for use in safety critical applications where any failure to perform (when properly used in accordance with any specification or instructions) can be reasonably expected to result in significant injury or death of user.

11. Supply of this document is governed by the laws of England and is subject to the exclusive jurisdiction of the courts of England.