

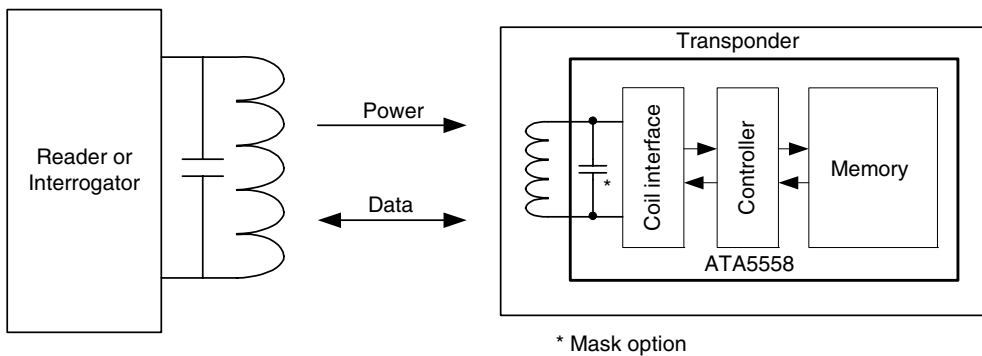
Features

- Contactless Read/Write Data Transmission
- Radio Frequency f_{RF} : 100 kHz to 200 kHz
- User Memory (1024 Bits): 32 Write Protectable 32-bit Blocks of Data
- Deterministic Anticollision: Detection Rate ~ 20 Tags/s with 40-bit Tag ID, RF/32
- On-chip CRC Generator: 16-bit CRC-CCITT Compliant to ISO/IEC 11785
- Downlink Transmission: Enhanced 1 out of 4 Pulse Interval Encoding (~ 5 kbps)
- Uplink Transmission: ASK Modulated, NRZ, Manchester or Bi-phase Encoding
- Integrated Tuning Capacitor: 75 pF $\pm 10\%$ as Mask Option
- System Memory (320 bits):
 - 10 Write and Password Protectable 32 Bit Blocks of Data
 - Tag ID (96 Bits Maximum)
 - Traceability Data with Inherent Manufacturer Serial Number
 - Write Password (32 Bits) and Read Password (32 Bits), with Page Orientated Memory Protection Areas
 - Configuration Register for Setup of:
 - Selectable Data Bit Rate: RF/2 .. RF/64
 - Selectable Tag ID Length to Optimize Anticollision Detection Rate
 - Start of Frame with Variable Preamble Length to Simplify Interrogator Design
 - Public Mode (PM) for Read Only Tag Emulation
 - Electrical Article Surveillance (EAS) Mode
 - Direct Data (NRZ), Bi-phase (FDX-B) or Manchester Data Encoding

1. General Description

The ATA5558 is a contactless, two-terminal R/W-Identification IC (IDIC[®]) for multi- or single tag applications in the low frequency (≈ 125 kHz) range. The passive tag uses the external RF signal to generate it's own power supply and internal clock reference.

Figure 1-1. RFID System Using an ATA5558 Tag



It contains an EEPROM which is subdivided into 1024 bits of user memory and 320 bits of system memory. Both memory sections are organized in data blocks of 32 bits, each equipped with an associated lock bit for block write protection. The user memory, which is intended for storage of recallable user data, is made of 32 such blocks. The 10 block system memory section is reserved for system parameter and configuration settings. Two of these blocks include a 32 bit read and a 32 bit write password to prevent unauthorized read and/or write access to protected user definable memory pages.



1 kbit R/W IDIC[®]
with
Deterministic
Anticollision

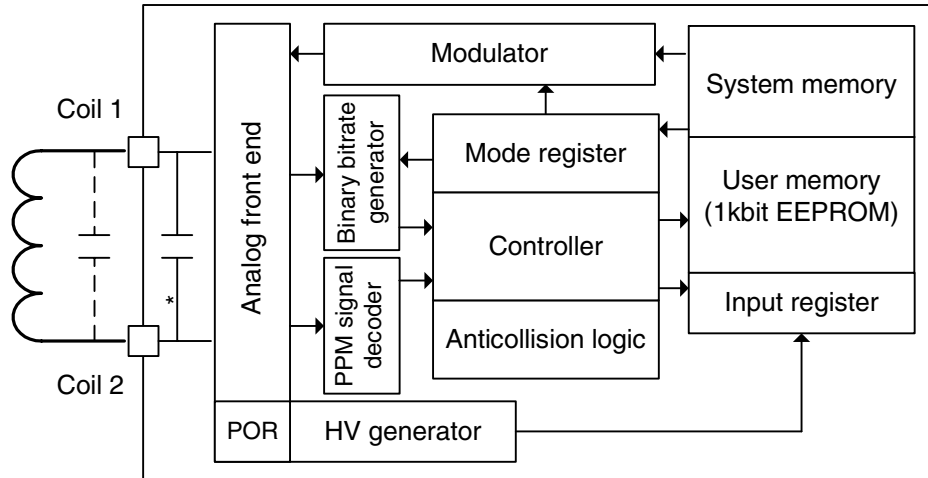
ATA5558

Preliminary



The ATA5558 receives commands from the interrogator (downlink) as a *1 out of 4* pulse interval encoded, amplitude modulated signal. Return data transmission from the tag to the interrogator (uplink) utilizes either Manchester, Bi-phase or NRZ encoded amplitude modulation. This is achieved by controlled damping of the interrogator's RF field with an on-chip resistive load between the two tag terminals, Coil 1 and Coil 2. Multi-Tag identification is implemented using a deterministic anticollision algorithm which requires unique tag identification information (Tag ID's). Three blocks within the system memory are reserved for storage of the Tag ID, the length of which is user configurable up to a maximum of 96 bits.

Figure 1-2. System Block Diagram



* mask option

2. Functional Blocks

2.1 Analog Front End

The analog front end (AFE) includes all circuitry directly associated with the coil interface. It generates the internal power supply and handles the data communication with the interrogator. It consists of the following blocks:

- Rectifier to generate a DC supply voltage from the AC coil voltage
- Low-voltage regulator to provide an on-chip stabilized DC voltage
- Charge pump to generate the high voltage required for EEPROM programming
- On-chip tuning capacitor (mask option)
- Field clock extractor
- Field gap detector for data transmission from interrogator to tag
- Load switching between Coil 1/Coil 2 for data transmission from tag to interrogator
- Electrostatic discharge protection (ESD)

2.2 Power-On Reset (POR) and Initialization

The Power-On-Reset circuit (POR) maintains the circuit in a reset state until an adequate internal operating voltage threshold level has been reached, whereupon a default start-up delay sequence is started. During this period of 200 field clock cycles, the configuration and security setup is initialized from the System Configuration and Page Security blocks.

2.3 Control Logic

The control logic is responsible for the following functions:

- Initialization and reloading of the configuration from EEPROM
- Control of read and write memory access operations
- Data transmission and command decoding
- CRC check, error detection and error handling

2.4 Modulator

The modulator output circuitry controls the switching of a resistive load between the Coil 1 and Coil 2 pads to transmit data from the tag to the interrogator (uplink). The ASK load modulator is driven from the Manchester, Bi-phase encoder or directly from the EEPROM memory data stream (NRZ) according to the uplink encoding configuration.

Table 2-1. Types of Modulation

Uplink Mode	Manchester Encoding	Bi-phase Encoding ⁽¹⁾	NRZ – Direct Data
ASK-coded modulation	0 = falling edge on mid bit 1 = rising edge on mid bit	0 = rising or falling edge 1 = no edge on mid bit	1 = modulation off 0 = modulation on

Note: 1. Since Bi-phase encoding is data dependent the following definitions apply to the ATA5558 implementation.

- The tag modulates the first (half) bit period after SOF.
- If the last bit of a data stream is a logical 1 it is possible that this bit period is non-modulated and therefore is not detectable directly by the reader.

Figure 2-1. Manchester Timing Diagram

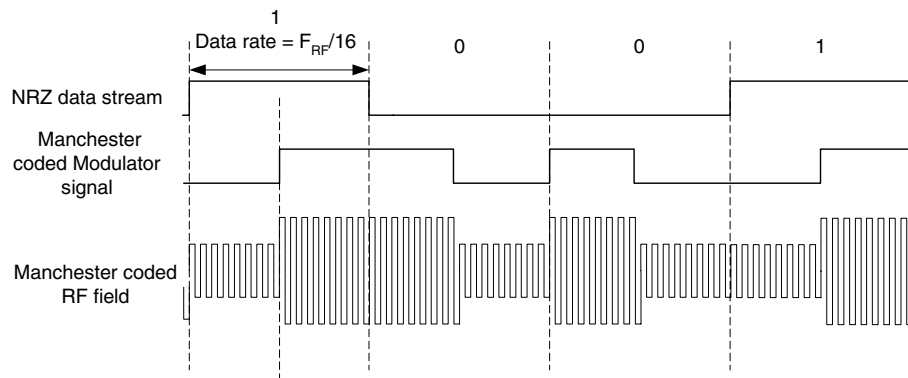
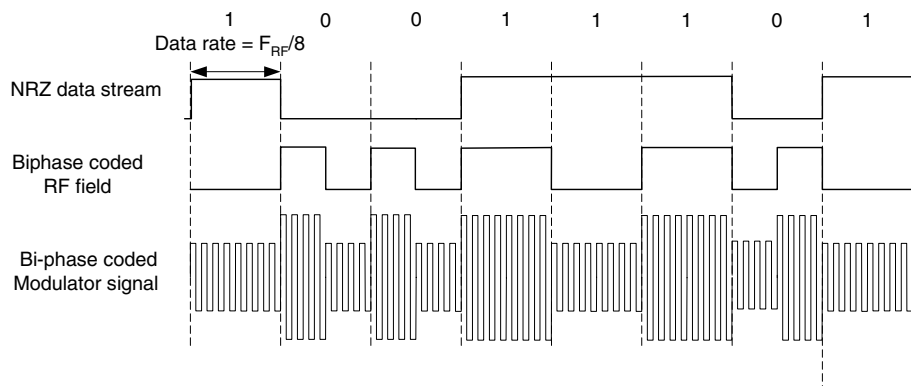


Figure 2-2. Bi-phase Timing Diagram



2.5 Binary Bit Rate Generator

The tag's data rate is binary programmable in the configuration register to operate at any bit rate between $RF/2$ and $RF/64$.

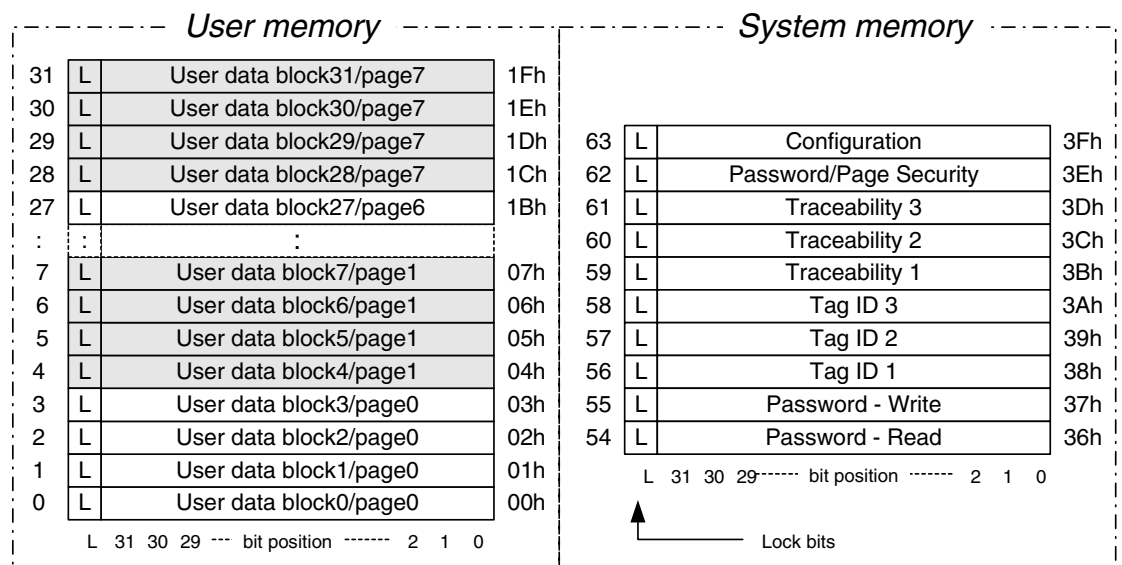
$$\text{Data rate} = \frac{RF}{2(n + 1)}$$

2.6 Memory Section

2.6.1 Memory Map

The physical memory is subdivided into two logical sections (see [Figure 2-3](#)). The first logical memory section contains the 1024 bits of user data. The second logical memory section contains 320 bits of system/configuration data. Both memories are organized in 32-bit data blocks, each block being equipped with a single lock bit, with which the associated block can be write protected. Command controlled programming and reading always takes place on a serial MSB first block basis so that a block constitutes the smallest directly accessible data unit. The user memory is further subdivided into 8 pages, each of 4 blocks in size. This provides the basis of the page security scheme ("[Password Protection](#)" on [page 6](#)).

Figure 2-3. Memory Map Structure



A valid Write command can be used for programming a data block of 33 bits – including the associated lock bit – into an addressed location of either memory section. Once locked (lock bit = 1), the entire block including the lock bit itself can no longer be reprogrammed selectively.

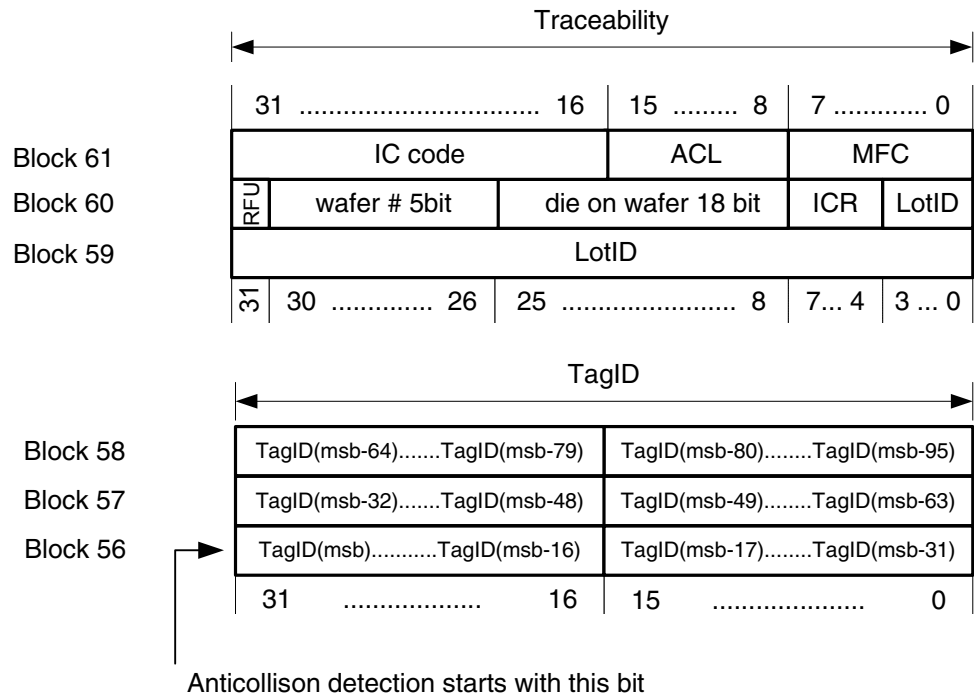
The system memory section is situated at the upper end of the (6-bit) memory address range and contains all system parameters and configuration settings. This area has restricted access (see Figure 2-5 on page 7) and the majority of blocks can only be read or written after the successful execution of the appropriate Password Login command (see Table 7-1 on page 24).

All the configuration settings are allocated in block 63 (see Figure 2-7 on page 9) and the password protection security information in block 62 (see Figure 2-6 on page 7).

2.6.2 Traceability Data

The traceability information is programmed and locked into the traceability blocks (59-61) by Atmel during the production test.

Figure 2-4. Tag ID and Traceability Structure



- IC code 4-digit Atmel IC reference number, e.g. '5558'
- ACL Allocation class as defined in ISO/IEC TDR 15963-1 = E0h
- MFC Manufacturer code of Atmel Corp. as defined in ISO/IEC 7816-6/AM1 = 15h
- ICR 4-bit Atmel IC revision code
- DPW 18-bit binary encoded die on wafer
- Wafer# 5-bit binary wafer number
- Lot ID 9-digit lot number
- RFU Reserved for Future Use

The blocks 59, 60 and 61 contain Atmel's manufacturer's serial number (MSN). The top 4 digits of block 61 specify the IC code of this product. The following byte of block 61 is fixed to E0h which is the allocation class (ACL) for registered IC manufacturers as defined in TDR 15963-1; followed by the manufacturer code (MFC), which compliant with ISO/IEC 7816-6/AM1, is defined as 15h for Atmel. The remaining two blocks contain a 64-bit Atmel unique traceability code. The data is divided in several sub-groups, a 36-bit lot ID code, a 5-bit wafer number and a 18-bit sequential die number which represents the physical location of the chip on the processed wafer. The ICR nibble (4 bits) of this manufacturer serial number (MSN) is used for the IC reference/version (ICR).

The unique tag identifier (Tag ID) blocks provide an address code with which each tag can be individually identified and interrogated. These codes are programmed by either the tag system administrator or the tag manufacturer into blocks 56 to 58. The allocation of individual Identification codes must be handled so that an interrogator can never be confronted with two tags with identical Tag IDs. This is an important issue as the Tag ID is used as the basis for accessing and sorting tags during anticollision commands *GetID*, *Select* and *SelectGroup*.

The Atmel traceability code (blocks 60 and 59) itself provides a means of unique chip identification so that this data content can be used as the Tag ID or a part of the Tag ID by copying it or part of it into blocks 56 and 57.

The Tag ID code is located in blocks 56 to 58. It is MSB aligned so that it may occupy between 16 and 96 bits (see [Figure 2-4 on page 5](#)). This Tag ID length is set in the configuration block (see [Figure 2-7 on page 9](#)) and has an impact on the time required to complete the anticollision detection loop so it should be adjusted to suit system requirements. The default preprogrammed Tag ID length is 64 bits. The anticollision algorithm is based on a bit by bit binary tree elimination, carried out in parallel on all the Tag IDs within the interrogator field. This starts with the MSB of the Tag ID (always in bit position 31 of block 56) and continues through to bit position 0 of block 58 or until the Tag ID LSB, indicated by the configuration Tag ID length, is reached.

2.7 Security Levels

The ATA5558 has three levels of security. Firstly, the restricted password access which prevents unauthorized access to both user and system data but allows authorized access using the correct password. Then a block orientated absolute write lock protection (lock bits) and finally the Master Key with a security code which has to be set in the configuration block accordingly (see [Table 2-2 on page 8](#) and [Figure 2-7 on page 9](#)).

2.7.1 Password Protection

The user memory is subdivided into continuous page areas which can be configured so that write or read/write and write operations on blocks within these pages can only be carried out after the appropriate password has been transmitted to the tag (LoginRead or LoginWrite command). The read and write password protections are independent and user definable. The read and write passwords are found in blocks 54 and 55 and the page security levels are defined in the Page Security register of block 62 (see [Figure 2-6 on page 7](#)).

To access a protected memory block, a Login command with the corresponding read or write password had to be executed once per session. During the login procedure the 32-bit password field of the login command is compared with the contents of the corresponding password in the system memory. If the passwords match, the ATA5558 tag will return an SOF pattern as an acknowledge signal. If they do not match, the tag will respond with an SOF followed by the appropriate error code. Writing to a protected memory address which has not been enabled with the correct LoginWrite password, will result in an error code on completion of the interrogator command. Reading a password protected memory address which has not been enabled with the correct LoginRead password, returns a block of all 0 data and no error code.

Figure 2-5. System Memory Access

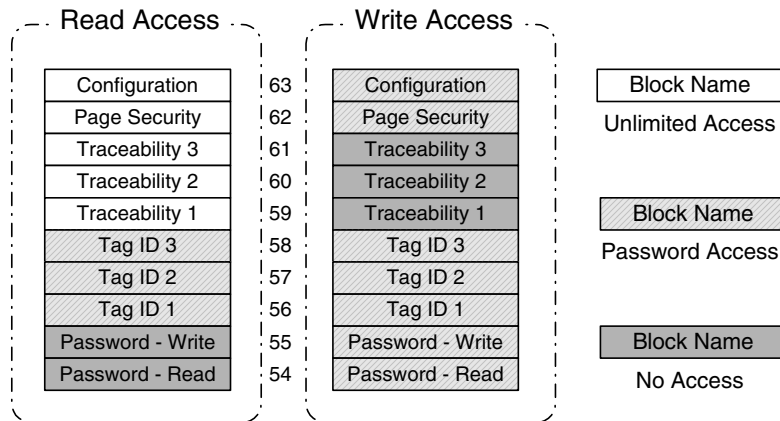
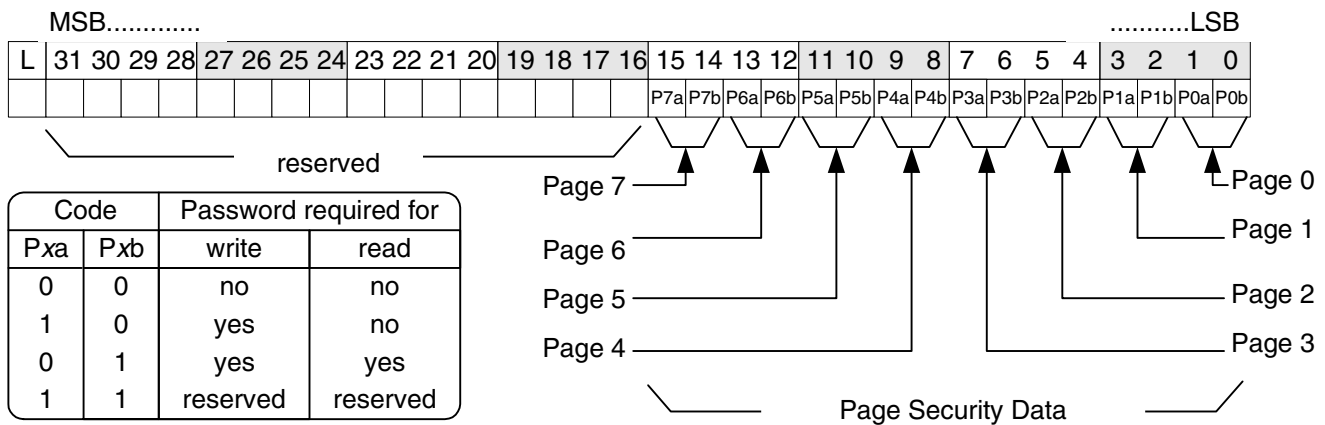


Figure 2-6. Page Security Register



2.7.2 Lock Bit

Each memory block, consists of 32 data bits and an associated lock bit (see [Figure 2-3 on page 4](#)). Once a block is locked (lock bit = 1), the entire block including the lock bit itself can no longer be reprogrammed

2.7.3 Master Key

The Master Key controls various operating modes as described in [Table 2-2](#). For production test purposes, other Master Key codes are used, but once the Configuration block has been double locked these test functions can never be reactivated.

If the Master Key is set to *0110*, the blocks within the system memory section have different access protection (see [Figure 2-5 on page 7](#)). These access rights are fixed and not influenced by the Page Security Register. Access to password protected system memory blocks can only be performed after the corresponding LoginWrite or LoginRead has been successfully executed. The password blocks themselves are non-readable. Traceability and configuration can always be read but the traceability data cannot be altered.

Table 2-2. Master Key Related Functions

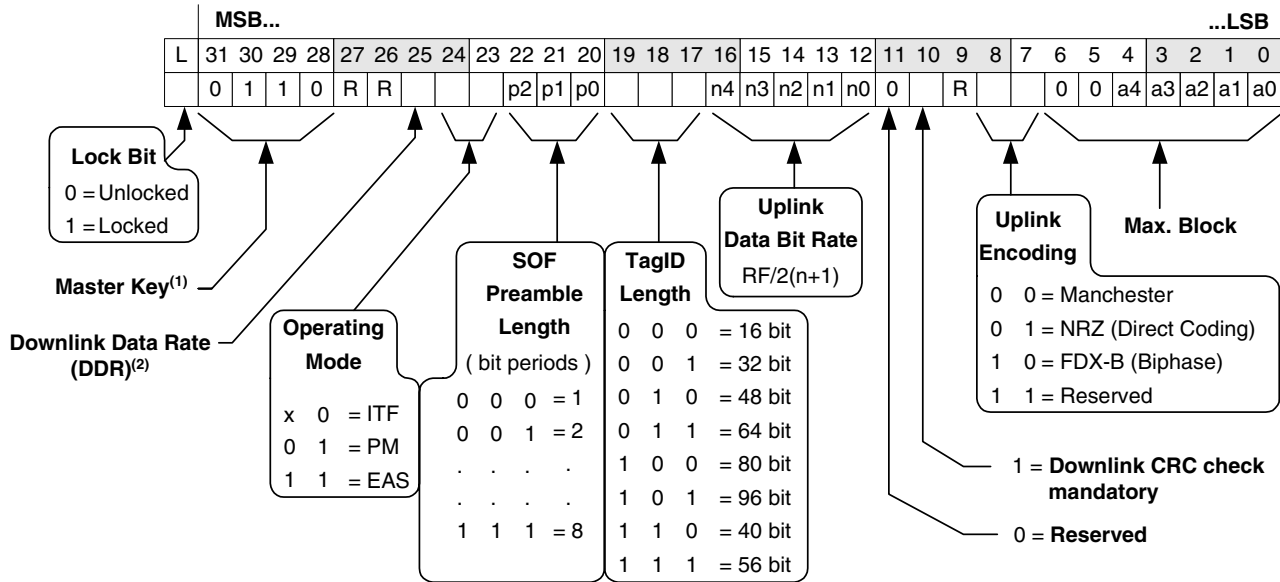
Master Key	Enables				Protection Scheme	
	DDR	PM	EAS	User Memory Clear	Page Security	System Memory
6	yes	yes	yes	no	yes	yes
9	yes	yes	yes	yes	yes	yes
others	no	no	no	yes	no	no

A new ATA5558 device, when received by the customer can be considered as being unprogrammed (all *0* state), the only exception to this being the preprogrammed non-alterable traceability information. For the tag manufacturer to be able to easily set up the tag passwords, it is possible to provisionally switch the password protection off. i.e Master Key = *0*. In this state, it is possible to read and write all non-locked (lock bits = *0*) memory blocks irrespective of the page security. In this way, new tag passwords or Tag ID's can be defined and written. Blocks, which have once been locked (block lock bit = *1*) can however not be rewritten. When the customer has completed the tag configuration, the Master Key is set to the "safe" state (= *6*) thus enabling the full password protection, and then finally the configuration block itself may be locked. In this double locked condition, the configuration and all other locked blocks are irreversibly set and cannot be changed. This applies to both the user and the majority of the system memory blocks.

2.8 Tag Configuration Register

The internal tag configuration register holds a shadow copy of the configuration settings stored in the system memory's block 63. It is refreshed after every POR cycle (RF field on), Reset to Ready or Write to block 63.

Figure 2-7. Configuration Register



Notes:
 (1) If master key = 6hex then all test modes are ignored and password protection enabled
 (2) If DDR = 1 and master key = 6hex or 9hex then data rate = fast, otherwise slow
 R = reserved for future use, should be set to 0
 x = don't care state

ITF = Interrogator Talks First Mode
 PM = Public Mode
 EAS = Electrical Article Surveillance
 NRZ = Non Return to Zero

3. Transmission Protocol

The transmission protocol defines the mechanism to exchange commands and data between the interrogator and the tags. In all but the Public and EAS Mode, the interrogator has complete control over the communication flow – all data transmission being synchronized to interrogator commands and the interrogator field clock – “Interrogator Talks First” (ITF) principle. This means that a tag does not transmit data, unless it has received and properly decoded an interrogator command.

The protocol is based on an exchange of

- commands from the interrogator to the tag (Downlink mode)
- and response from the tag to the interrogator (Uplink mode)

3.1 Tag to Interrogator Communication

All transmissions from the tag to the interrogator utilize amplitude modulation (ASK) of the RF carrier. This takes place by controlled switching of a resistive load between the coil pads which in turn modulates the RF field generated by the interrogator.

The tag is capable of communicating with the interrogator via inductive coupling. Typical examples of the incorporated amplitude modulation is shown in [Figure 3-1](#):

- Manchester encoded data signal
- Bi-phase encoded data signal
- NRZ direct data encoding
- Dual pattern data coding is used during the anticollision loop and for an error code response

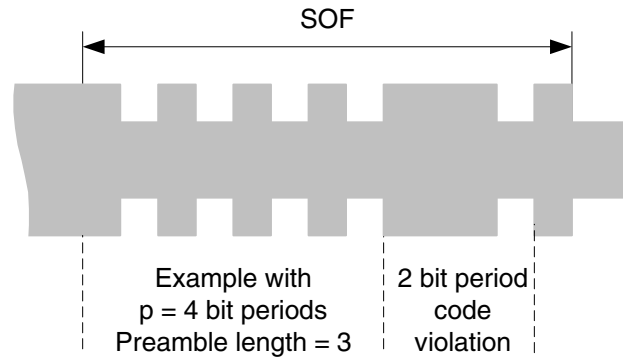
Figure 3-1. Tag to Interrogator - Load Modulation Coding

NRZ Data	Normal Manchester data coding	Normal Biphase data coding	Anticollision dual pattern data coding
Data "1"	<p>Diagram showing Normal Manchester data coding for Data "1". The load is off for the first half of the bit duration T_d and then switches to on for the second half.</p>	<p>Diagram showing Normal Biphase data coding for Data "1". The load is on for the first half of the bit duration T_d and then switches to off for the second half.</p>	<p>Diagram showing Anticollision dual pattern data coding for Data "1". The load is off for the first half of the bit duration T_d, then on for the second half, and then off for the third half.</p>
Data "0"	<p>Diagram showing Normal Manchester data coding for Data "0". The load is on for the first half of the bit duration T_d and then switches to off for the second half.</p>	<p>Diagram showing Normal Biphase data coding for Data "0". The load is off for the first half of the bit duration T_d and then switches to on for the second half.</p>	<p>Diagram showing Anticollision dual pattern data coding for Data "0". The load is on for the first half of the bit duration T_d, then off for the second half, and then on for the third half.</p>

3.1.1 Start of Frame (SOF) Encoding

After the reception of a valid interrogator command the tag will reply immediately with a Start of Frame (SOF) pattern. The SOF pattern is made up of a variable length preamble and a fixed 2-bit (Manchester) code violation followed by a half bit duration of unmodulated carrier. The preamble length as set in the configuration block defines the number of (Manchester coded) zero initialization data bits. If the preamble length in the configuration register is set to zero, a single start bit will precede on the code violation.

Figure 3-2. SOF Pattern



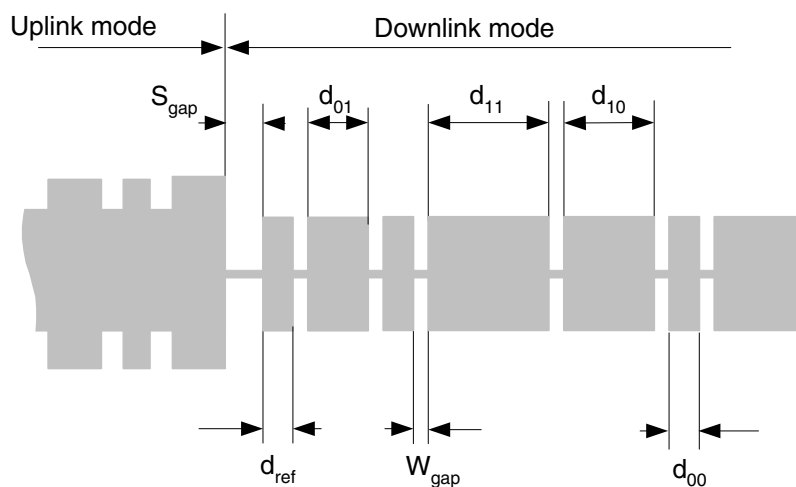
3.1.2 Public Mode

1. In Public Mode the cyclic data stream will be preceded by a single SOF pattern after the completion of the POR delay.
2. The variable number of preamble data bits is aimed at easing the interrogator design and optimizing system performance.
3. Within any closed identification system the preamble length for all tags must be identical.

3.2 Interrogator to Tag Communication

All commands and data bit streams from the interrogator to the tag are 100% (OOK – On-Off-Key) modulated using a modified 1 out of 4 pulse position coding. Depending on the data, the continuous RF field is interspersed with short field gaps of constant duration and variable separation. The time from one gap to the next may take on one of four discrete values. Each of these represent one of four possible dual bit downlink data codes (00 .. 11) in the data stream (see [Figure 3-3](#)). The downlink data transfer speed is dependent on the downlink data rate (DDR) bit set in the tag configuration block, so that selected tags can always understand the interrogator. The minimum write data coding (maximum data rate) is 9 field clocks. This corresponds with the d_{00} (d_{ref}) parameter in [Figure 3-3](#) and [Table 3-1](#) on page 12.

Figure 3-3. Interrogator to Tag - Modified 1 out of 4 Pulse Position Coding



3.2.1 Start Gap

The first command gap is usually slightly longer (~20 field clocks) than the following data gaps. This is referred to as the start gap. All interrogator to tag commands are initiated by such a start gap. As soon as the clock extractor detects a start gap, the tag's receive damping is switched on. This serves to improve the gap detection of all following data gaps.

A start gap can be detected at any time after the completion of the tag's power on reset delay sequence (RF field-on plus ~3 ms). If a gap is received during this delay sequence, irrespective of whether it is part of a command or a start gap, the delay will be restarted. Commands or partial command sequences occurring during the power on reset sequence will not be executed.

3.2.2 4PPM Command Encoding

The timing between data gaps depends on the Downlink Data Rate (DDR) in the configuration register and is nominally 9 or 13 field clocks for a 00, 17 or 29 field clocks for a 01, 25 or 46 field clocks for a 10 and 33 or 61 field clocks for a 11. The duration of the field gaps themselves lie between 8 and 20 field clocks. Should no gap be detected for more than the maximum 11 gap separation (see Table 3-1), the tag(s) will terminate the present command decoding mode and, if enabled, release the receive damping. If an error is detected within the command sequence (e.g. incorrect number of bits received, CRC check failed etc.) the tag will return a dual pattern coded error to the interrogator and ignore the command. The first two bits of every command constitute the Start of Command (SOC) and is always 00. This SOC is used as a timing reference for all following data (see Table 3-1), thus providing an auto-adjustment to allow for varying environmental conditions.

Table 3-1. Modified Pulse Position Modulation - Timing Parameters

Parameter	Remark	Symbol	DDR = 1 and Master Key = 6 or 9			DDR = 0 or Master key ≠ 6 or 9			Unit
			Min.	Typ.	Max.	Min.	Typ.	Max.	
Start gap		S_{gap}	8	10	50	8	10	50	T_c
Write gap		W_{gap}	8	10	20	8	10	20	T_c
Write data coding (gap separation)	Reference data 00	d_{ref}	9	–	68	13	–	72	T_c
	00 data	d_{00}	$d_{ref} - 3$	d_{ref}	$d_{ref} + 4$	$d_{ref} - 7$	d_{ref}	$d_{ref} + 8$	T_c
	01 data	d_{01}	$d_{ref} + 5$	$d_{ref} + 8$	$d_{ref} + 12$	$d_{ref} + 9$	$d_{ref} + 16$	$d_{ref} + 24$	T_c
	10 data	d_{10}	$d_{ref} + 13$	$d_{ref} + 16$	$d_{ref} + 20$	$d_{ref} + 25$	$d_{ref} + 32$	$d_{ref} + 40$	T_c
	11 data	d_{11}	$d_{ref} + 21$	$d_{ref} + 24$	$d_{ref} + 28$	$d_{ref} + 41$	$d_{ref} + 48$	$d_{ref} + 56$	T_c

- Notes:
1. All absolute times assume $T_c = 1/f_c = 8 \mu s$ ($f_c = 125 \text{ kHz}$)
 2. All the above timing data is that which should appear on the device terminals so that the device can operate correctly. Depending on the coil used (e.g. Q factor etc.) and the transmission medium, the values implemented in the interrogator could differ slightly.

Figure 3-4. Command "Read Block #23"

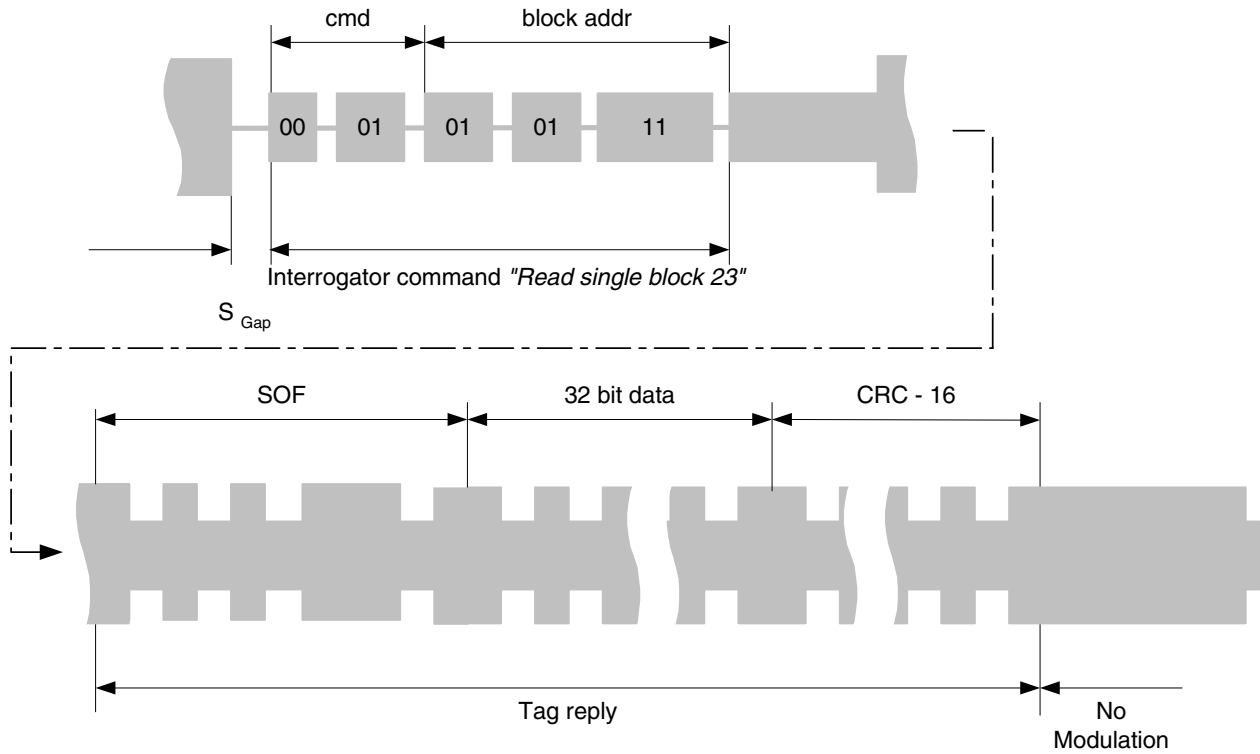
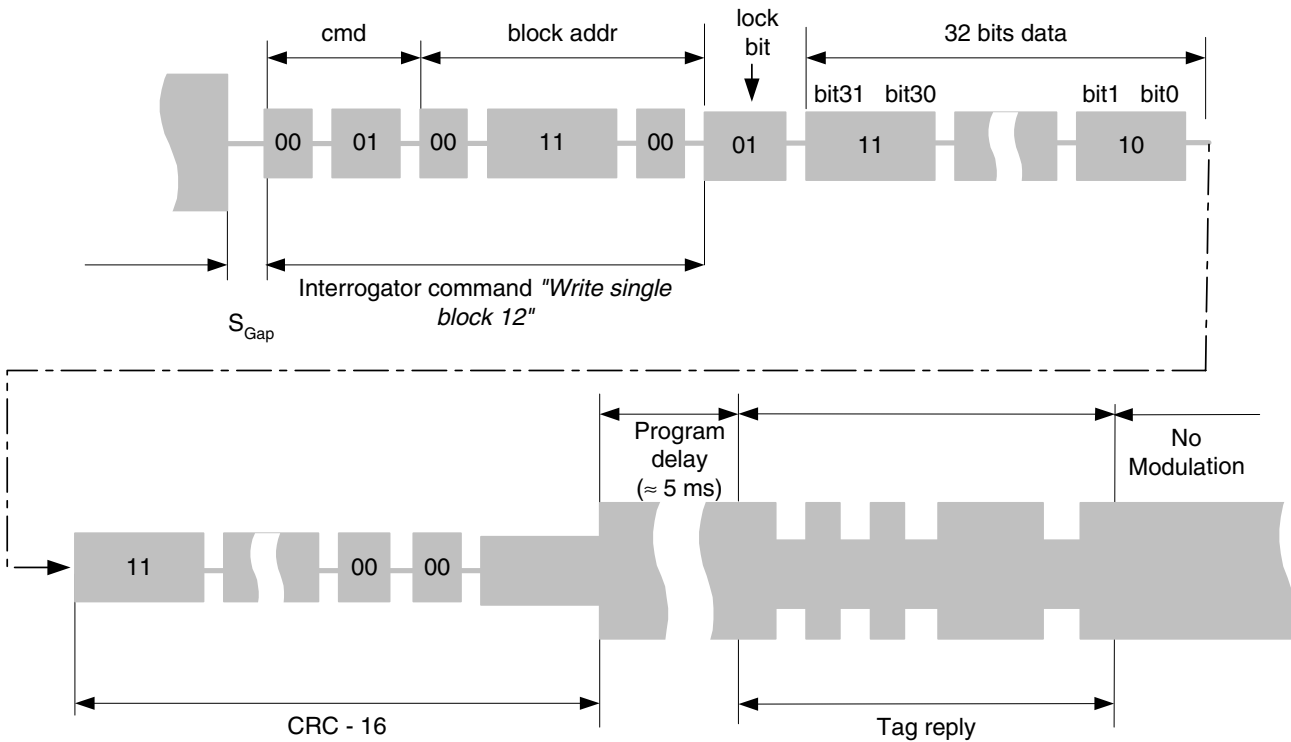


Figure 3-5. Command "Write Block #12"



4. CRC Error Checking

The CRC error checking circuitry generates a 16-bit CRC to ensure the integrity of transmitted and received data packets. The ATA5558 uses the CRC-CCITT (Consultative Committee for International Telegraph and Telephone) for error detection. The 16 bit cyclic redundancy code is calculated using the following polynomial with an initial value of $0x0000$:

$$P(X) = x^{16} + x^{12} + x^5 + x^0$$

The implemented version of the CRC check has the following characteristics:

- Reverse CRC-CCITT 16 as described in ISO/IEC 11785
- The CRC 16-bit shift register is initialized to all zeros at the beginning of a command
- The incoming data bits are XOR-ed with the MSB of the CRC register and is shifted into the register's LSB
- After all data bits have been processed, the CRC register contains the CRC-16 code.
- Reversibility - The original data together with associated CRC, when fed back into the same CRC generator will regenerate the initial value (all zero's).

Should a CRC be required, both the tag and interrogator must use the above CRC polynomial. During read/write operations, a CRC can be attached to information by either the interrogator and/or the tag

In the case of downlink communication, a CRC (CRC_d) can be attached to information transmitted from the interrogator to the tag(s) (see [Figure 4-2 on page 15](#)). This is evaluated by the tag(s) to ensure correct transmission.

During the uplink phase of the read commands the tag replies with the requested data block(s) followed by an uplink CRC (CRC_u). This CRC_u is generated in the tag's CRC generator, from the downlink address, CRC_d (if used) and the returned data (see [Figure 4-3 on page 16 a, b, c](#)). So by initializing the interrogator's CRC generator with the same address and CRC_d (if used), then subsequently updating it with the returned data and uplink CRC_u, the integrity of both the address understood by the tag and data itself can be verified. On receiving a response from the tag which includes a CRC_u, it is recommended that the interrogator verifies this. If it is found to be incorrect, the interrogator should take the appropriate actions. These actions are left to the discretion of the system designer.

During the anticollision detection, the CRC can also be used as a means of tag identification. A tag which is successfully selected by one of the select commands or as the result of an anticollision elimination cycle, will always reply with a CRC. This is generated from it's own Tag ID (see [Figure 4-3 on page 16 d](#)) and is always preceded by an SOF pattern. This also provides an additional means of double checking whether the intended tag has been selected.

For any write command, if the bit 10 of the configuration register = 1, the usage of the CRC for this communication is mandatory. Failure to include or verify a CRC results in the tag aborting the command execution and returning an error code. If the configuration register bit 10 = 0, the Write CRC usage is optional. In this case, the CRC is handled in the same manner as a read command i.e. the CRC is only evaluated if attached. Should no CRC be transmitted and the configuration register bit 10 = 0, then the command will always be executed.

Figure 4-1. Schematic Diagram of CRC Generation

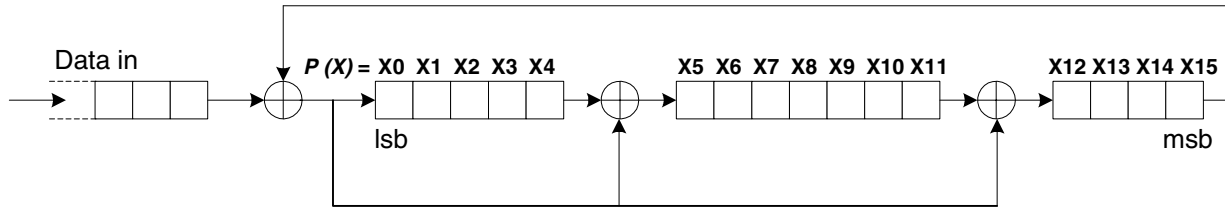


Figure 4-2. Examples of Downlink CRC Generation

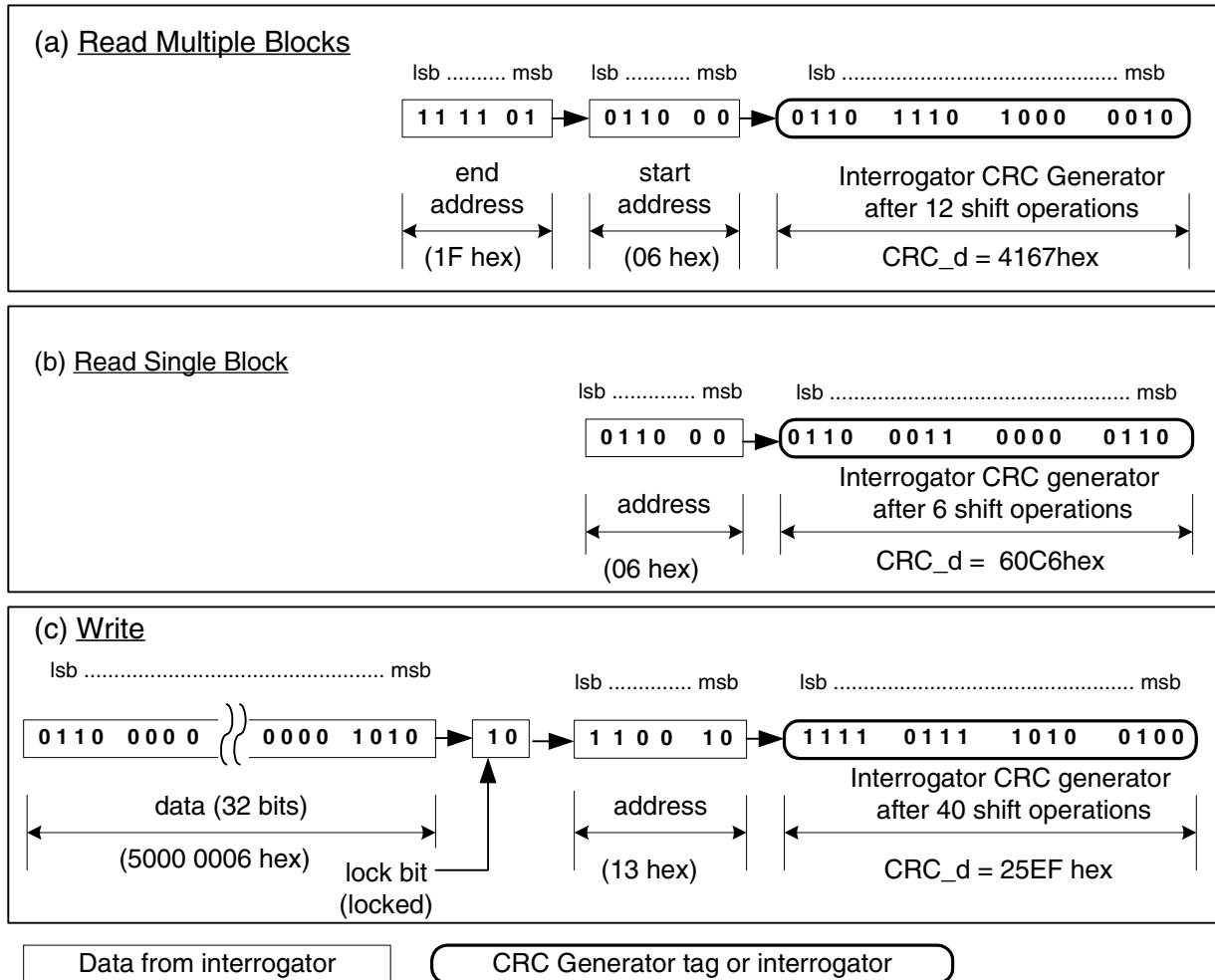
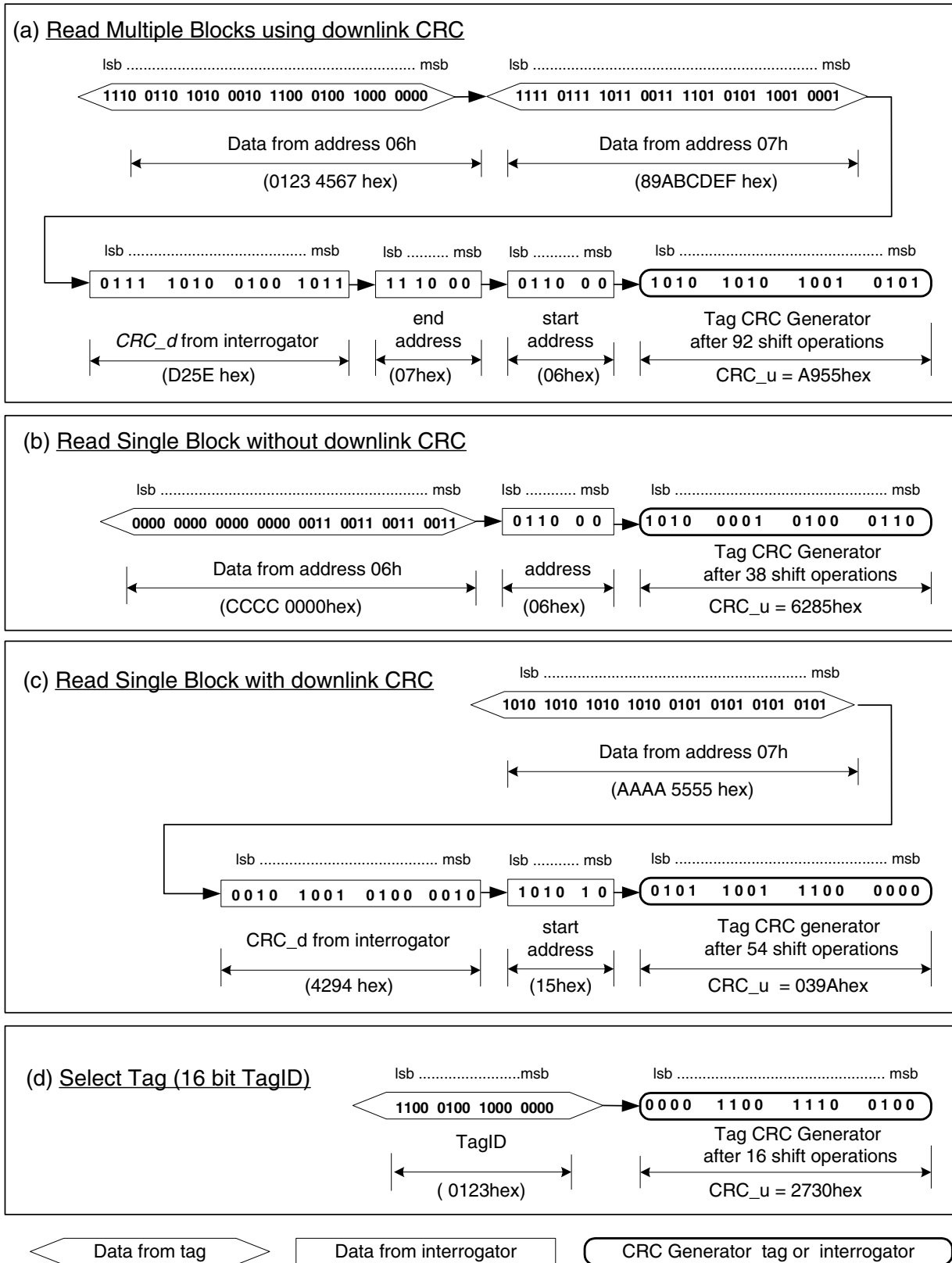


Figure 4-3. Examples of Uplink CRC Generation



5. Operating Modes

After initialization, the Operating Mode (Configuration block bits 23 and 24) is interrogated and depending on its state, the device will go into either the READY state of the “Interrogator Talks First” (ITF) mode or the Public Mode’s PM READY state if the PM bit is set or the “Electronic Article Surveillance” (EAS) mode is selected.

5.1 Interrogator Talks First Mode (ITF)

For multi-tag applications, the ATA5558 is used in the “Interrogator Talks First” (ITF) mode with anticollision handling capability. In this mode, the tag starts up in the READY state, where it remains silent and waits for further interrogator commands before communication can take place.

5.2 Tag State Machine

Any tag can find itself in one of the following states:

- POWER DOWN
- PM READY (for PM or EAS modes only)
- READY (ITF mode)
- SELECTED
- QUIET

In the state diagram shown in [Figure 5-1 on page 18](#), a state transition takes place by applying or removing the field (power on/off) or via one of the commands Select, SelectAll, SelectGroup, ResetSelected or ResetToReady. When a tag is unable to decode or process an interrogator command (e.g. CRC or bit frame error), it will remain in the current state. Depending on the state, tag(s) will only accept certain commands.

5.3 Power Down State

The tag is in the Power Down state when there is not enough energy in the interrogator field to activate the tag. The ATA5558 commences a power-on initialization delay with an activated weak damping level to achieve a field strength threshold for stable operation.

5.4 READY State (ITF)

The ATA5558 tag enters the READY state after it has been activated by the interrogator (RF-field on) or after receiving either a ResetToReady or ResetSelected command (the EAS and PM deactivated). The READY state is the initial anticollision state, and in general all tags on this state are unidentified.

5.5 Selected State

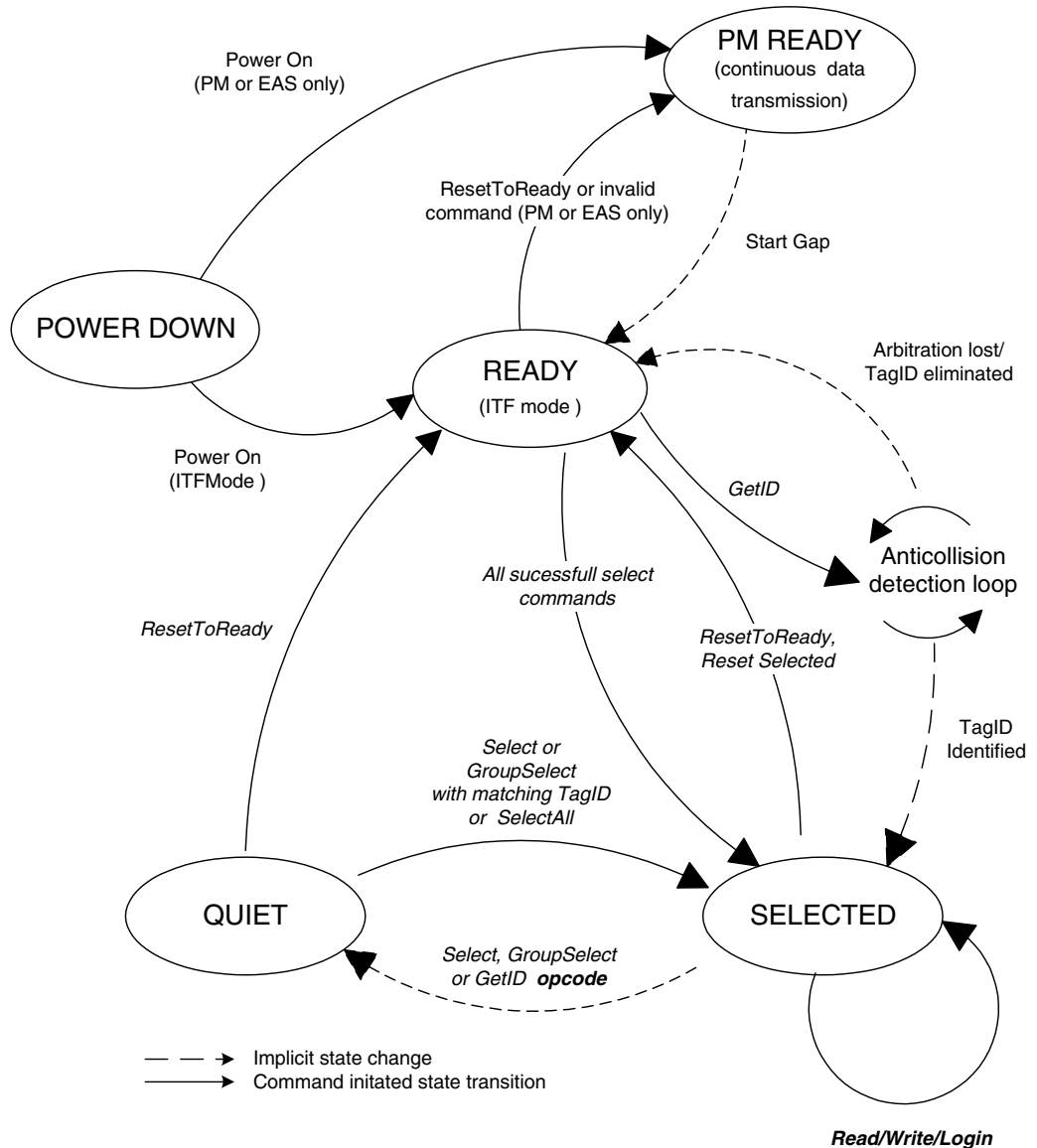
Before a tag can in any way be accessed, it must first be selected. Tag selection can take place individually in which case they find themselves within the Selected state. They can enter the Selected state as a result of receiving an explicit Select command with the matching Tag ID. In this way, only one tag can theoretically be in the Selected state at any one time. If a tag should find itself in the Selected state and a second tag is selected by a subsequent Select command, the first tag will automatically proceed into the Quiet state.



It is possible to carry out commands simultaneously on more than one tag. To do this they must all first be selected by specifying a group of tags within the READY state and putting the group into the Selected state. This is performed by using a SelectGroup command with a matching partial Tag ID pattern. A group of tags in the Selected state may be written simultaneously with identical blocks of data. Data verification and checksum errors are reported by the tags using a special dual pattern code. Tags within the Selected state will automatically drop into the Quiet state and be excluded from subsequent anticollision detection, if a subsequent Select or GetID command is received.

Selection can also take place on tag groups with non-matching Tag ID patterns using the SelectNGroup command. This could be useful for example, to check a storage crate for items which do not match a certain selection criteria (e.g. color or dispatch destination), so a SelectNGroup command with the Tag ID mask set to the color black will GroupSelect all non-black items. If no tag responds with a SOF pattern, then there are no black items present.

Figure 5-1. Tag State Diagram



5.6 Quiet State

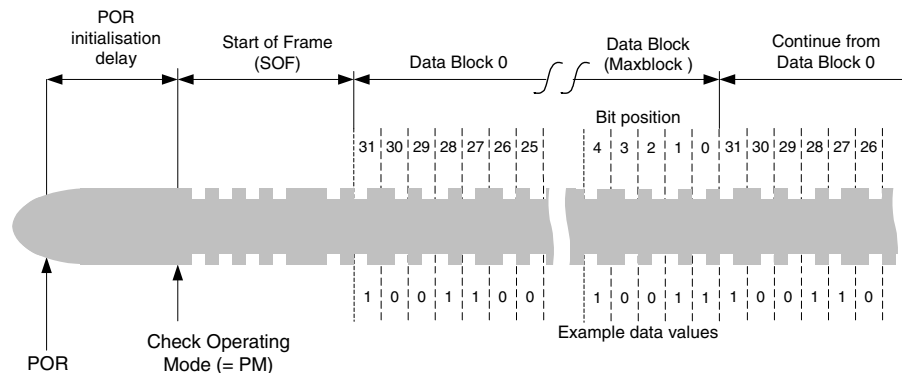
The tag goes into the Quiet state from the Selected state when a new selection takes place i.e. a Select or a GetID command is received. Unlike the READY state, the tag's Tag ID in this state is known. Tags in the Quiet state are excluded from subsequent anticollision detection.

5.7 Public Mode (PM) and PM READY State

In the Public Mode, communication commences with a single "Start of Frame" pattern (SOF), followed by a continuous stream of serialized user data which is read cyclically from the user memory. This starts with block 0, bit 31 and continues sequentially through to bit 0 of the final block address defined by the configuration parameter MAXBLOCK. After reaching the MAXBLOCK address, data transmission repeats with block 0, bit 31. If, for example MAXBLOCK were set to 1, block 0 and 1 would be continuously transmitted. This transmission process continues indefinitely until terminated by either switching the field off or on the receipt of a valid interrogator command.

On the start of a new command the tag will proceed temporarily from the PM READY state into the (ITF) READY state. If the command is valid, it will be executed and the tag state changes as if in the ITF mode (see Figure 5-1 on page 18). If the command is invalid, then it will drop back into the PM READY state and continue to transmit data. To restart the public mode transmission, the tag must be re-initialized by reapplying the field (POR) or by using a ResetToReady command.

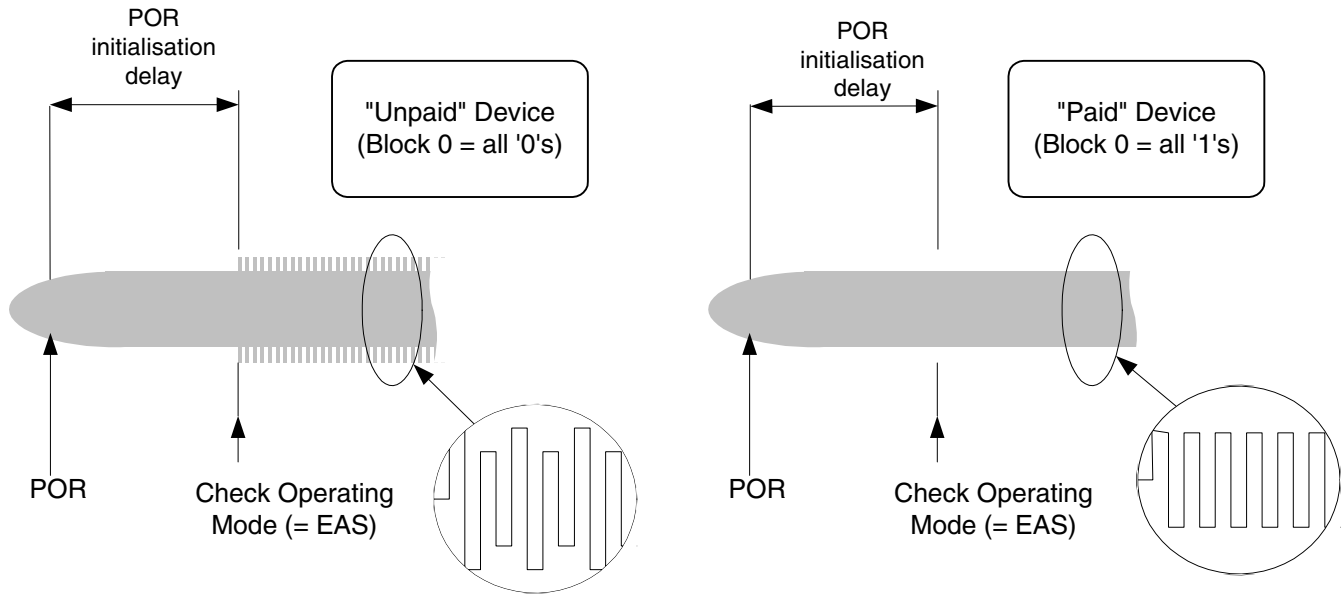
Figure 5-2. Public Mode Start Up



5.8 Electronic Article Surveillance (EAS)

The EAS Mode is intended for retail article surveillance whereby the device will be physically attached to retail articles in a store or supermarket. The device will be preprogrammed into an "unpaid state" before entering the sales area by programming the block 0 to MAXBLOCK of the user memory to all 0s. For convenience reasons MAXBLOCK should be set to 0 in the configuration word. To increase security, the memory pages containing block 0 to MAXBLOCK should be assigned a write password security level (see password protection). Once the article has been purchased at the cash desk, the device is programmed into a "paid state" by writing the block 0 with all 1 s, using the appropriate password (if necessary). As soon as an "unpaid" device enters an interrogator field, it will modulate the interrogator field with an RF/2 signal. This can be detected by the surveillance interrogator and used to trigger an appropriate audio or visual warning. A "paid" device will remain silent. As in the Public Mode, the device will revert to ITF mode READY state as soon as it receives a valid interrogator command. By reapplying the field (POR) or using a ResetToReady command, the device returns to EAS mode.

Figure 5-3. EAS Startup



6. Anticollision Protocol

The aim of the anticollision protocol and associated arbitration process is to detect and identify the Tag ID's of all tags within the READY state which are present within range of the interrogator field.

The interrogator masters all communication with single or multiple tags. Tag arbitration communication is initiated by issuing the GetID command. All tags in the READY state will then enter the anticollision detection loop and synchronously start to transmit an identification response that represents the tag's individual unique Tag ID code. Using an iterative bit-wise sorting algorithm on these Tag ID's, the interrogator is capable of eliminating all but one tag. This remaining tag is thus selected and can be accessed directly by following commands. Tags eliminated during the detection loop are muted, drop back into the READY state to participate in the next detection cycle.

A typical anticollision procedure is illustrated in the following scheme:

a) The interrogator starts the anticollision detection by sending a GetID command.

Any previously eliminated and muted tag will be put into the READY state. All tags in the READY state participate initially in the anticollision detection loop.

If nothing is known of the Tag ID's within range, then the GetID command includes no further parameters and the detection group encompasses all tags. After a predefined number of field clock cycles, all tags within range reply by synchronously transmitting a SOF pattern followed by their own respective Tag ID(MSB).

Anticollision detection can be reduced to a subgroup of tags by passing a partial Tag ID pattern as Tag ID command parameter. These bits represent the most significant bits of the Tag ID subgroup. Anticollision detection will then be carried out on this subgroup, continuing as above with the synchronous reply from all constituent tags, followed by their most significant unknown Tag ID bit(s).

- b) The interrogator can detect whether any tag is present.

If no SOF pattern is returned then there is no tag present within the detection group so the process continues with (a).

- c) The interrogator checks the tag responses bit-wise within the anticollision loop.

If one or more active tags are within range, the interrogator will sequentially scan the Tag ID bits from the most significant through to the least significant bits. Each time slot corresponds to a particular Tag ID bit position. All tags reply simultaneously with dual pattern modulated data, the response signals being superimposed on one another. A damped signal will thus overwrite a non-damped signal so that a logical 1 Tag ID bit will prevail over a logical 0 bit.

- d) The interrogator checks and eliminates tags.

If the interrogator detects a Tag ID logical 1 bit, it acknowledges reception by broadcasting a gap in the field signal. This can be monitored and evaluated by all tags within the detection group. Otherwise a Tag ID logical 0 bit induces no reaction from the interrogator.

On observing an acknowledge gap, any individual tag can, by checking the state of its own current Tag ID bit, deduce whether it should remain in the current anticollision detection loop (Tag ID bit = 1) or whether it should eliminate itself from the detection group (Tag ID bit = 0).

Eliminated tags will be muted and fall back into the READY state where they take no further part in the current detection loop. They remain in this state until the next anticollision loop is started by a new GetID command. Continue to (a)

Non eliminated tags remain in the detection loop and if the final Tag ID bit has not been reached then the next Tag ID bit is interrogated in (c) otherwise (e).

- e) End of a single anticollision loop

By the time the final Tag ID bit has been interrogated, there will be only one remaining active tag within range – all others having been eliminated during the previous interactions. Assuming no new tags have entered the interrogation since the start of the anticollision loop and that all the signals have been correctly interpreted, the interrogator should at this stage be able to identify the associated Tag ID. This active tag is set automatically into the Selected state and replies with the anticollision response which consists of an SOF followed a 16 bit CRC generated from its own Tag ID. If the received CRC matches the Tag ID the interrogator may continue with (a) or (f).

If the received CRC is corrupted or does not match the calculated 16 bit value the interrogator will issue a ResetSelected command to transfer this improperly selected tag back into the READY state. Continue to (a).

- f) The interrogator communicates directly with tag in Selected state.

At this stage the single identified and selected tag can undergo direct communication with the interrogator and can be read and written with either Read, Write or Login commands. This tag remains selected until the interrogator starts a new anticollision loop with a new GetID command, or if other tags are addressed directly using a Select or GroupSelect command. The selected tag then drops into the Quiet state where it is excluded from all future anticollision detection loops. Continue to (a).



Figure 6-1. Anticollision Loop

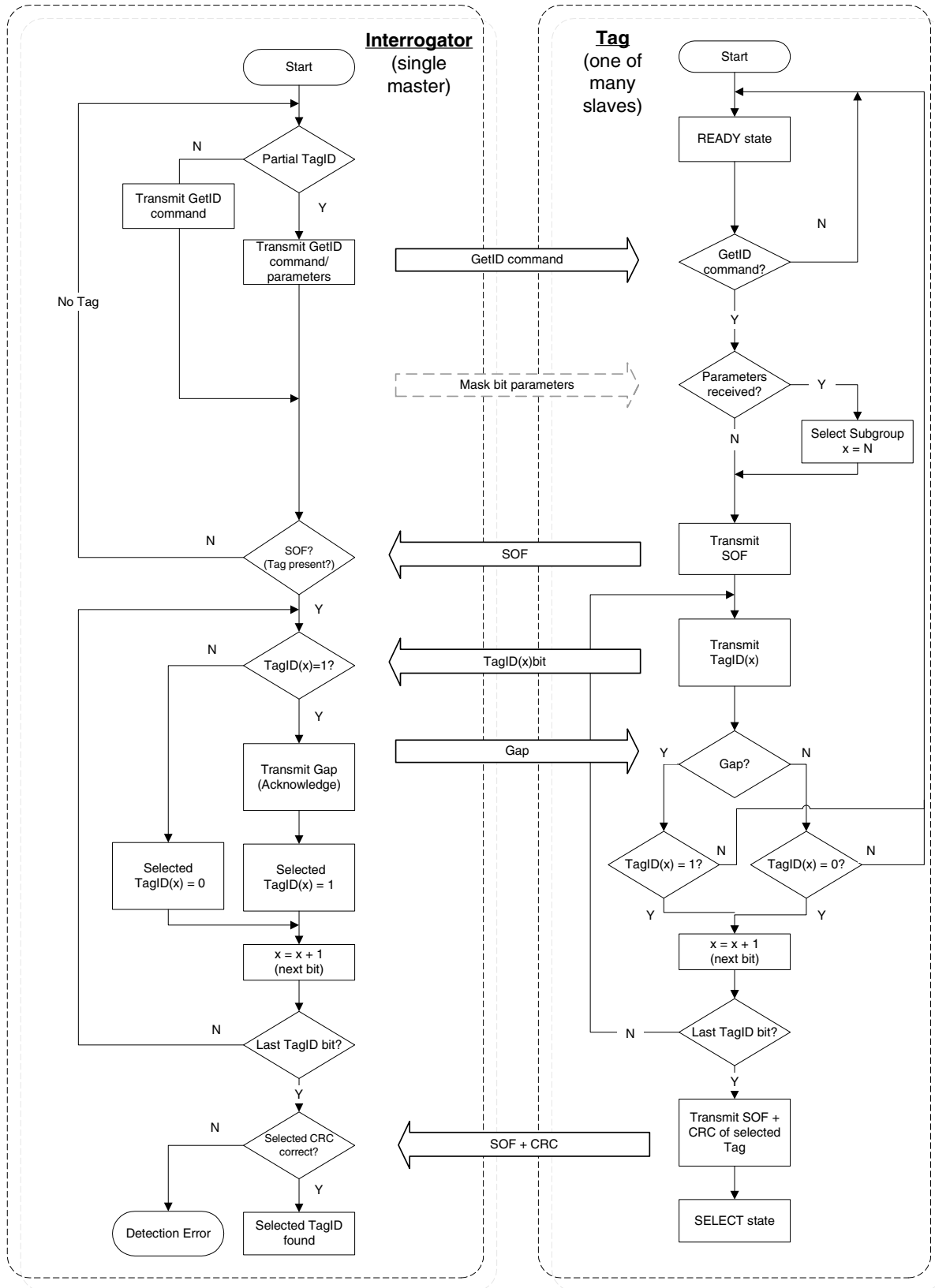


Figure 6-2. GetID Command with Partially Known Tag ID

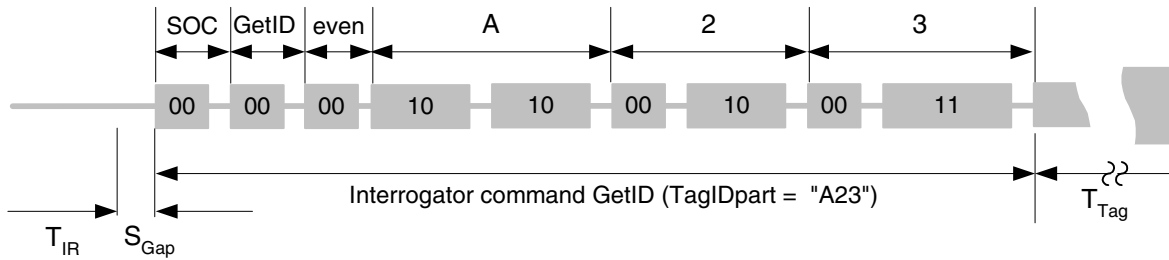


Figure 6-3. Subsequent Tag Responses in Anticollision Loop (Two Alternative Tag IDs)

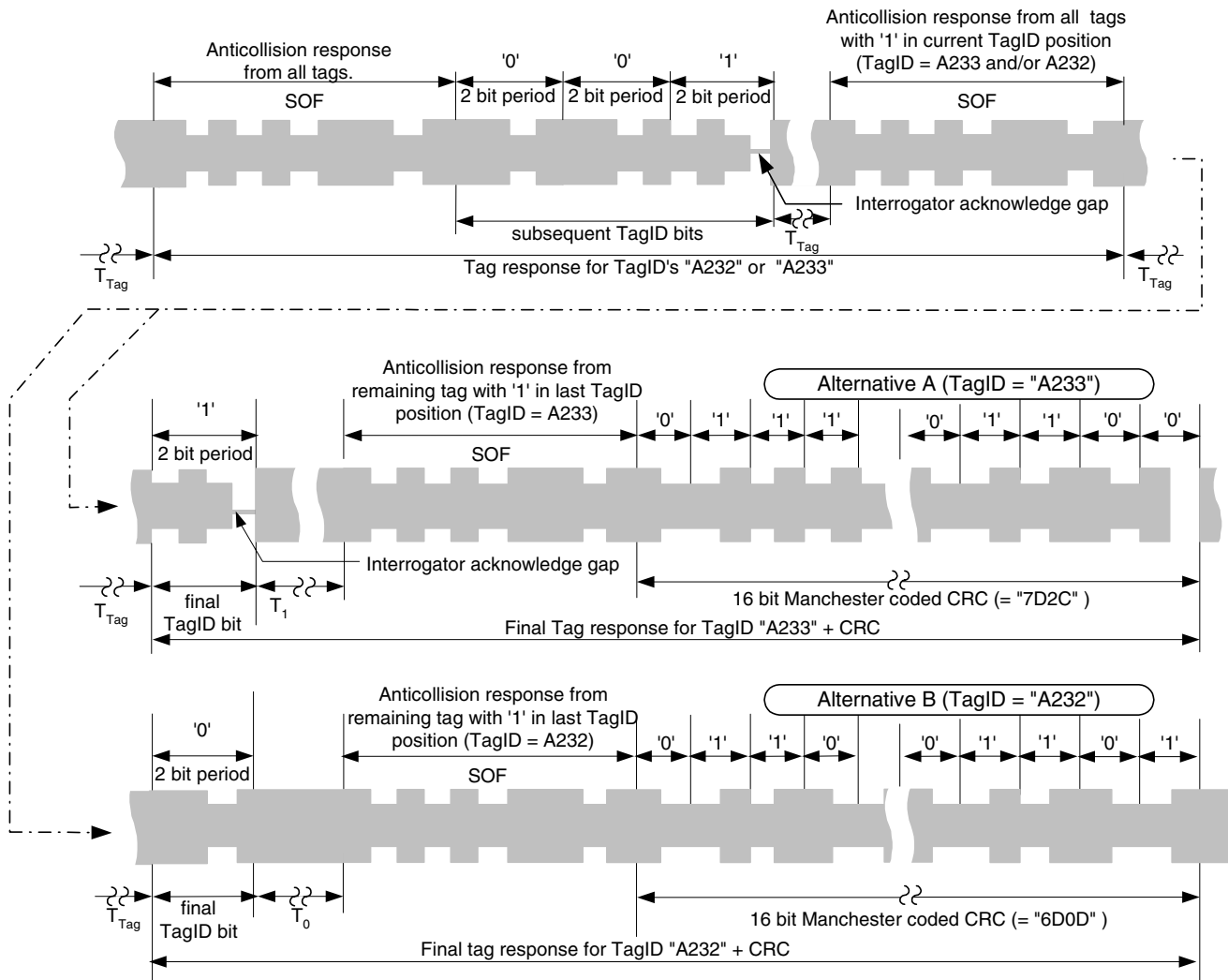


Table 6-1. Anti-collision Timing

Parameter	Remark	Symbol	Formula	$T_{Bit}=f_C/32$		Unit
Tag reaction time	End of start gap to start of tag command processing	T_{IR}		≥ 0		T_C
Tag to Interrogator response time	End of final command gap to start of tag SOF acknowledge	T_{Tag}	$d_{11,max} + 1\frac{1}{2} \times T_{Bit}$ (see Figure 4-1 on page 15)	DDR = 1	84	T_C
				DDR = 0	116	T_C
End of anticollision loop to start of SOF (and CRC) response	Final bit of Tag ID = 0	T_0	$2 \times T_C + 1\frac{1}{2} \times T_{Bit}$		50	T_C
	Final bit of Tag ID = 1	T_1	$= T_{Tag}$	DDR = 1	84	T_C
				DDR = 0	116	T_C

Note: In the above example the following is assumed: $f_C = 125$ kHz; $T_C = 1/f_C = 8$ μ s and a data rate of $f_C/32$; so a bit period $T_{Bit} = 32 \times T_C$

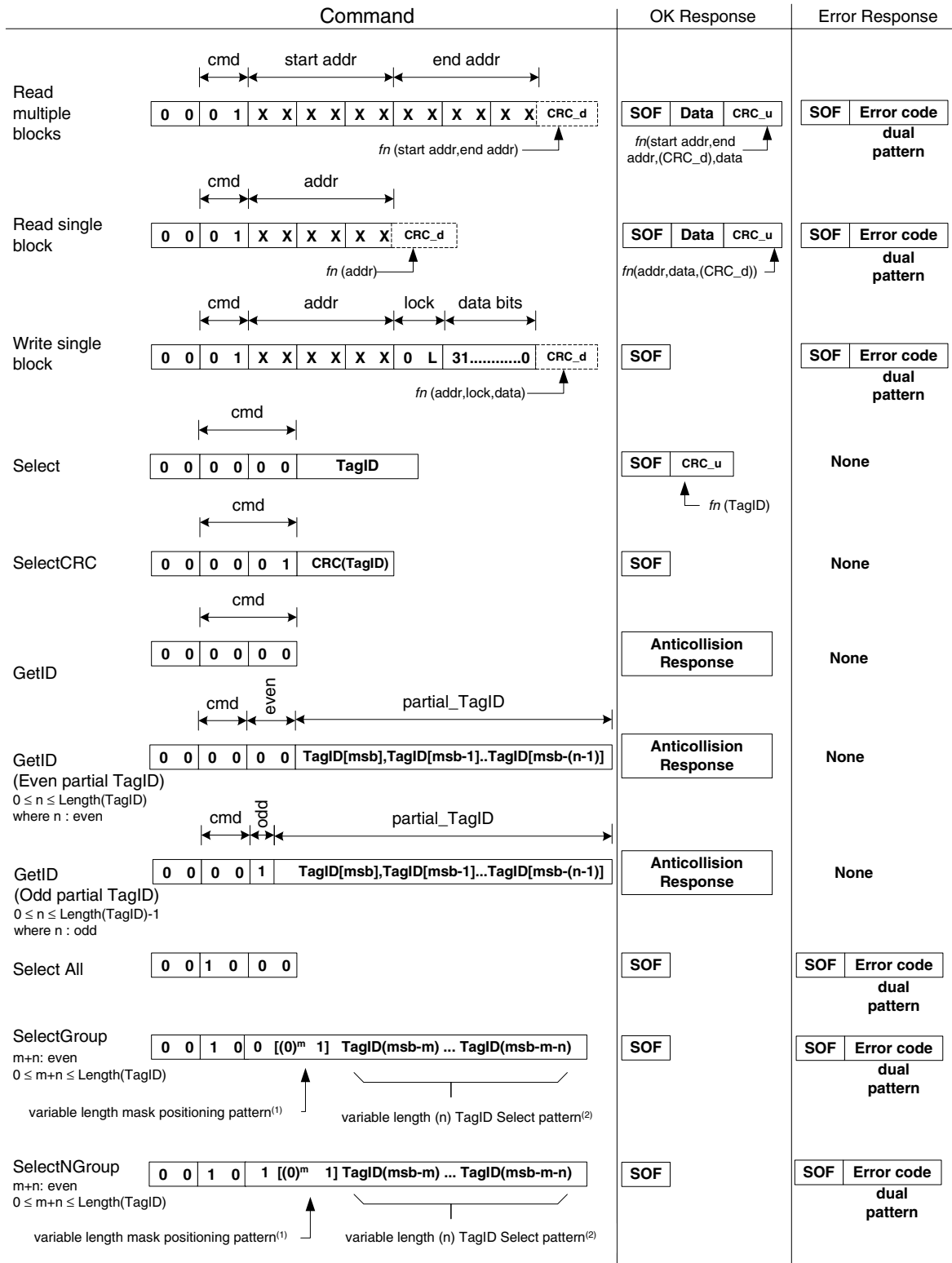
7. Command Set

The first two bits of any interrogator command are called Start Of Command (SOC) and are always 00. This pulse interval is used for auto calibration purposes. The following series of dual bit packets define the interrogator command opcodes and the command dependant parameter information. A command overview is given in [Table 7-1](#) below

Table 7-1. List of ATA5558 Supported Commands

Command	SOC	Opcode	Number of Parameter bits	Description
Read Single Block	00	01	6 (+ 16 CRC_d)	Read single 32 bit data block and CRC_u (+ optional downlink CRC_d)
Read Multiple Blocks	00	01	12 (+ 16 CRC_d)	Read multiple data blocks and CRC_u (+ optional downlink CRC_d)
Write Single Block	00	01	40 (+ 16 CRC_d)	Write a single block (+ optional downlink CRC_d)
Login Write	00	01 11 01 11 10	32	Login for write PWD protected access
Login Read	00	01 11 01 10 10	32	Login for read PWD protected access
GetID	00	00 00	None	Starts a complete new anticollision loop
GetID (Tag ID-part, even)	00	00 00	Length of partial Tag ID	Anticollision loop with partial Tag ID, with even number of matching Tag ID bits.
GetID (Tag ID-part, odd)	00	00 1	Length of partial Tag ID	Anticollision loop with partial Tag ID, with odd number of matching Tag ID bits.
Select (Tag ID)	00	00 00	Length of Tag ID	Puts specified tag into Selected state
SelectAll	00	10 00	None	Selects all tags in the RF field
SelectGroup	00	10 0[0]n 1	Length of Tag ID mask	Select a specific group of tags
SelectNGroup	00	10 1[0]n 1	Length of Tag ID mask	Select all tags which are NOT members of the specified group
ResetSelected	00	11 10 00 00	None	Reset selected tag to READY state without reloading configuration register
ResetToReady	00	11 00 00 00	None	Reset all tags in the RF field to READY state and reload configuration register from system memory (block #63)
ArmClear	00	11 00 10 00	6×0	Arms tag for ClearAll command
ClearAll	00	01 01 11 11	34×0 (+ 16 CRC_d)	Clears memory except traceability data (with optional constant CRC_d = 96ADh)

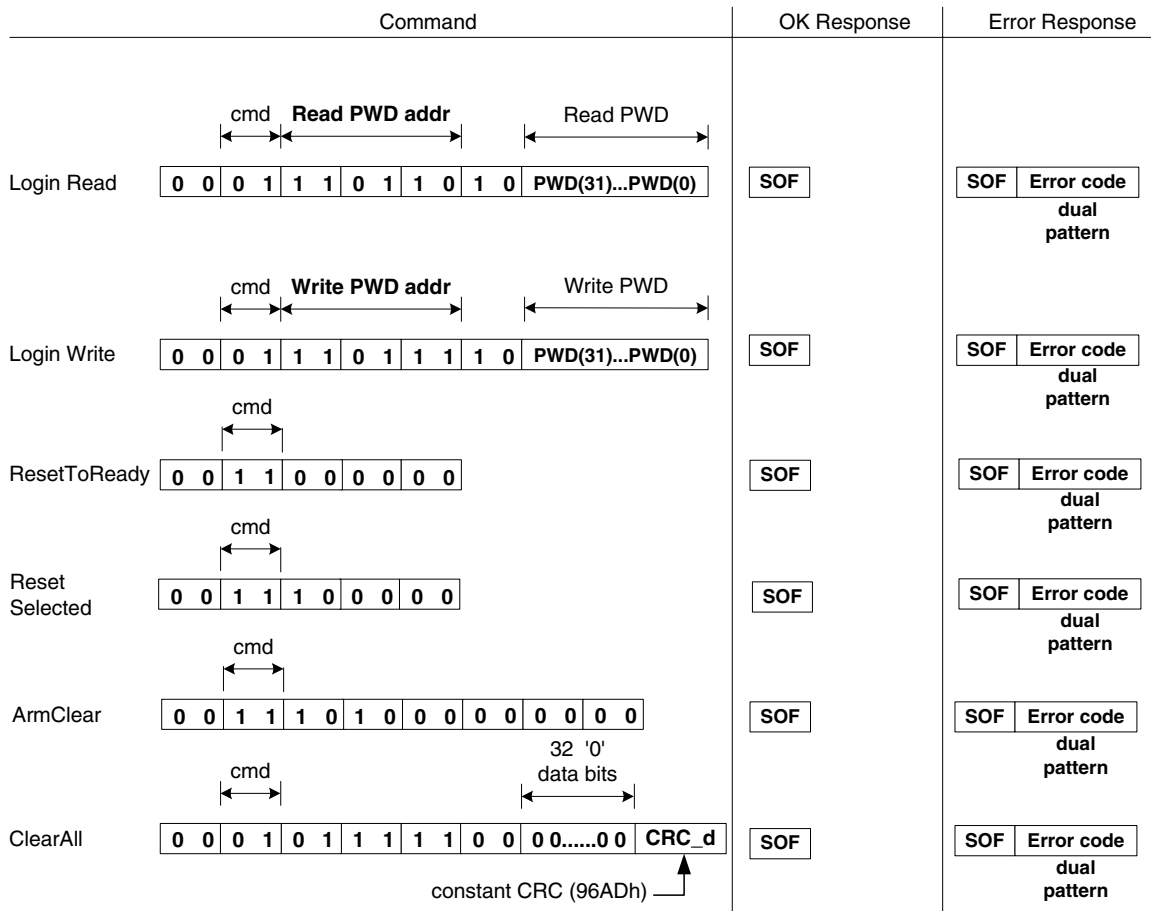
Figure 7-1. Command Format



- Note: 1. The leftmost position of the TagID select mask is determined by m '0' bits followed by a single '1' bit. These bit positions can be regarded as don't care bit positions.
- Note: 2. The TagID select mask is a variable (n) bits long. It starts immediately after the positioning pattern and can be terminated as required with the end of the command. All TagID lsb bits not defined are don't care.



Figure 7-2. Command Format (Continued)



7.1 Error Response

If a command sequence is in any case invalid, the tag answers immediately with one of the error codes (see [Table 7-2](#)). This is made up of an SOF pattern followed by a 4-bit dual pattern coded data word.

Table 7-2. Error Codes

Error Code	Description
0 1 1 1	Command format error – incorrect number of bits
1 1 1 0	Corrupt command (1 out of 4) encoding
0 0 1 0	Attempt to write a locked block – write command aborted
0 1 0 0	Attempt to write a protected block without a login – write command aborted
1 0 0 0	Login/Write command format error
1 1 0 1	Incorrect Login password
1 0 1 1	CRC error in command stream – command aborted
1 0 1 0	Program 0 verification error – unreliable zero level (degraded data retention)
0 1 1 0	Program 1 verification error – unreliable one level (degraded data retention)
others	Reserved for future use

7.2 Read Single Block

A Read Single Block command is executed on a tag in the Selected state. It serially reads a complete 32-bit tag data block. A downlink CRC (CRC_d) can be optionally included. This acts as a check for the block address. If included, the tag will always check the CRC_d and abort the command if it not compatible with the received address. If omitted, the tag will perform no downlink CRC check.

The tag responds to a single block read command with the requested 32-bit data block which is always followed by a 16-bit uplink CRC (CRC_u) to ensure data and address integrity. A read protected or non-existent memory block will return a block of 1 data bits (FFFF FFFF). A successful execution of a LoginRead command is necessary before reading a protected memory block.

It should be noted that the 16-bit CRC_u is generated from both the block address parameter and retrieved data. So that it acts as a check for the complete command transaction. From the received CRC_u, the interrogator can ensure that the data is correct and that it was read from the correct requested block address.

Table 7-3. Interrogator Command Parameters

Command	Parameter 1	CRC (optional)
Read Single Block = 00 01	Block Address	CRC_d (Block Addr)
4 bits	6 bits (MSB first)	16 bits (MSB first)

Table 7-4. Tag Response

SOF	Data	CRC
Start of Frame	Data Block	CRC_u (Block Addr + [CRC_d ⁽¹⁾] + Data)
3 .. 10-bit periods	32 bits (MSB first)	16 bits (MSB first)

Note: 1. optional

7.3 Read Multiple Blocks

A Read Multiple Blocks command is executed on a tag in the Selected state. It serially reads an array of consecutive 32-bit tag data blocks from a start address through to and including an end address. A downlink CRC (CRC_d) can be optionally included. This acts as a check for both block address parameters. If included the tag will always check the CRC_d and abort the command if it is not compatible with the received addresses. If omitted, the tag will perform no downlink CRC check.

The tag responds to a read command with the requested 32-bit data blocks which are always followed by a single 16-bit uplink CRC (CRC_u) to ensure data and address integrity. A read protected or non-existent memory block will return a block of 1 data bits (FFFF FFFF). A successful execution of a LoginRead command is necessary before reading a memory array including protected memory blocks.

It should be noted that the 16 bit CRC_u is generated from both the address parameters and retrieved data so that it acts as a check for the complete command transaction. From the received CRC_u, the interrogator can ensure that the data is correct and that it was read from the correct requested block address range.

Table 7-5. Interrogator Command Parameters

Command	Parameter 1	Parameter 2	CRC (optional)
Read = 00 01	Start Block Address	End Block Address	CRC_d (Start Block Addr + End Block Addr)
4 bit	6 bits (MSB first)	6 bits (MSB first)	16 bits (MSB first)

Table 7-6. Tag Response

SOF	Data	CRC
Start of Frame	Multiple Data Blocks	CRC_u (Start Block Addr + End Block Addr + [CRC_d*] + Data)
3 .. 10-bit period	$((\text{EndAddr} - \text{StartAddr} + 1) \times 32)$ bits (MSB first)	16 bits (MSB first)

7.4 Write Single Block

The Write Single Block command only effects tag(s) which have been previously been put in the Selected state. It performs the programming of a specific block address with a 32-bit block of data and associated lock bit. For password protected memory blocks the LoginWrite command has to be executed first, otherwise the programming will fail and an error code will be returned. Memory blocks which have a 1 in the lock bit are locked and cannot be written. The command protocol includes downlink CRC (CRC_d) which is used to check the downlink address and data. This CRC_d can be mandatory or optional depending on the state of bit 10 of the configuration register. If set to 1, the CRC_d must always be included and correct for the data programming to take place. If set to 0, the CRC_d is optional i.e. it is only checked if the CRC data is present.

On receiving the Write command, and if necessary checking the CRC_d, the tag will start the EEPROM programming sequence. The maximum EEPROM program time per block (including the lock bit) is 6 ms. This programming cycle includes an automatic read verification phase which makes sure that the data has been programmed securely thus ensuring satisfactory long term data retention. To signal the completion of a successful programming cycle, the tag returns a single SOF pattern.

If for any reason the programming of the data block fails, the tag will generate the corresponding error code. The error code bits are dual pattern coded (see [Figure 3-1 on page 10](#)) and preceded by a SOF pattern. An attempt to write to a locked block address or a downlink CRC error causes an immediate abort of the programming cycle followed by the transmission of the corresponding error response. In the case of an EEPROM data verification failure, the error response is returned after the completion of the programming cycle.

Table 7-7. Interrogator Command Parameters

Command	Parameter 1	Parameter 2	Parameter 3	CRC ⁽¹⁾
Write Single Block = 00 01	Block Address	0 + Lock bit	Write Data	CRC_d (Block Addr + Lock + Data)
4 bits	6 bits (MSB first)	2 bits	32 bits (MSB first)	16 bits (MSB first)

Note: 1. The downlink CRC (CRC_d) must be appended if bit 10 of the configuration register = 1, otherwise it is optional.

Table 7-8. Tag Response

SOF	Error Flags
Start of Frame	Present on error only
3 .. 10-bit period	4-bit – dual pattern code

7.5 LoginRead

The purpose of the LoginRead command is to release the read protection on all read protected data blocks within the user memory. A tag in the Selected state will respond with a SOF pattern if the transmitted read password matches the data stored in the tag's system memory block 36hex (Read PWD). In the case of a non-matching read password the tag will reply with a SOF pattern followed by an error code. After a successful LoginRead command, all read protected memory blocks may be read normally. This positive login status remains valid until a new tag is selected or the tag is reset.

Table 7-9. Interrogator Command Parameters

Command	Parameter 1	Parameter 2	Parameter 3
LoginRead = 00 01	11 01 10 (36hex)	10	Read Password
4 bits	6 bits (MSB first)	2 bits	32 bit (MSB first)

Table 7-10. Tag Response

SOF	Error Flags
Start of Frame	Present on error only
3 .. 10-bit period	4-bit – dual pattern code

7.6 LoginWrite

The purpose of the LoginWrite command is to release the write protection on all write protected data blocks within the user memory. A tag in the Selected state responds with a SOF pattern if the transmitted write password matches the data stored in the tag's system memory block 37hex (Write PWD). In the case of a non-matching write password the tag will reply with an SOF followed by an error code. After a successful LoginWrite command any write protected memory block may be modified, as long as the addressed memory block is not already locked. The positive login status is valid until a new tag is selected or the tag is reset.

Table 7-11. Interrogator Command Parameters

Command	Parameter 1	Parameter 2	Parameter 3
LoginWrite = 00 01	11 01 11 (37hex)	10	Write Password
4 bits	6 bits (MSB first)	2 bits	32 bits (MSB first)

Table 7-12. Tag Response

SOF	Error Flags
Start of Frame	Present on error only
3 .. 10-bit period	4-bit – dual pattern code



7.7 ResetSelected

A ResetSelected command will set all currently selected tag(s) back into the ITF mode's READY state. The tag(s) answers with a SOF pattern and will be able to participate in future anticollision sequences.

If either PM or EAS is enabled, this command will not return a selected back into public Mode Ready State ,i.e., the device will not start to transmit public mode data.

Table 7-13. Interrogator Command

Command
ResetSelected = <i>00 11 10 00 00</i>
10 bits

Table 7-14. Tag Response

SOF
Start of Frame
3 .. 10 bit-period

7.8 ResetToReady

In ITF mode, a ResetToReady command will set all tags within range of the RF field back into the Ready state. If either PM or EAS is enabled, the ResetToReady will set the tag back into the PM Ready state where it will start to transmit PM data. All tags will answer with the SOF pattern. In READY state they can then participate in future anticollision sequences.

The ResetToReady command reloads the configuration register from system memory block #63.

Table 7-15. Interrogator Command

Command
ResetToReady = <i>00 11 00 00 00</i>
10 bits

Table 7-16. Tag response

SOF
Start of Frame
3 .. 10-bit period

7.9 Select

When receiving a Select command, the addressed tag responds with the 16 bit CRC of the Tag ID and immediately enters the Selected state.

After selection, the interrogator may communicate with the selected tag using any valid Read, Write or Login commands. If the interrogator sends a new GetID or Select (another tag) command, the currently selected tag enters the Quiet state automatically.

Table 7-17. Interrogator Command Parameters

Command	Parameter
Select = 00 00 00	Tag ID
6 bits	<Length (Tag ID)> bits (MSB first)

Table 7-18. Tag Response

SOF	CRC
Start of Frame	CRC_u (Tag ID)
3 .. 10-bit period	16 bits (MSB first)

7.10 GetID

When receiving a general GetID command, all tags in the READY state will enter the anticollision loop and take part in the deterministic arbitration sequence. All activated tags will reply synchronously with the same anticollision response. This specific anticollision signature consists of a SOF pattern followed by subsequent dual pattern coded Tag ID bit(s) as illustrated in [Figure 3-1 on page 10](#) and [Figure 6-3 on page 23](#).

Table 7-19. Interrogator Command

Command
GetID = 00 00 00
6 bits

Table 7-20. Tag Response

SOF	Subsequent Tag ID Bit(s)
Start of Frame	Dual pattern code
3 .. 10-bit period	<n> × 2 bits periods (MSB first)

7.11 Get_ID (Partial Tag ID)

Any anticollision loop starts with the interrogator's GetID command. All tags in the READY state with a matching partial Tag ID will reply synchronously with their own personal anticollision response. This consists of an initial SOF pattern followed by the Tag ID bit(s) in dual pattern coding which continue until the complete Tag ID has been sent or until the tag is eliminated from the search.

Table 7-21. Interrogator Command Parameters (Even Number of (n) Known Tag ID Bits)

Command	Parameter
GetID (Tag ID) = 00 00 00	Tag ID [MSB], Tag ID [MSB-1],.....Tag ID[MSB-(n-1)]
6 bits	<n> bits (MSB first); where n = 2, 4, 6, 8....

Table 7-22. Interrogator Command Parameters (Odd Number of (n) Known Tag ID Bits)

Command	Parameter
GetID (Tag ID) = <i>00 00 1</i>	Tag ID[msb], Tag ID[msb-1],.....Tag ID[MSB-(n-1)]
5 bits	<n> bits (MSB first); where n = 1, 3, 5, 7, ..

Table 7-23. Tag Response

SOF	Subsequent Tag ID bit(s)
Start of Frame	Dual pattern code
3 .. 10-bit period	<m – n> × 2 bits periods

7.12 SelectAll

When receiving the SelectAll command, all tags in the READY state will enter the Selected state and answer with the SOF pattern. This allows the rapid global configuration and personalization of a collection of tags without having to select and program each tag sequentially.

Table 7-24. Interrogator Command

Command
SelectAll = <i>00 10 00</i>
6 bits

Table 7-25. Tag Response

SOF
Start of Frame
3 .. 10-bit period

7.13 SelectGroup

When receiving the SelectGroup command, all tags in the READY state with the matching partial Tag ID will enter the Selected state and answer with the SOF pattern. The partial Tag ID can vary in length. It's pattern position relative to the Tag ID is set by the first (leftmost) **1** in the command parameter. The preceding **0** bits act solely as "don't care" spacer bits. This "mask header" is not part of the actual partial Tag ID. The mask pattern follows the mask header and is terminated by the end of command.

Example of SelectGroup Parameters:

Sample Tag ID 6CB9 : *01 10 11 00 10 11 10 01*

The above Tag ID would be selected by all the following GroupSelect command parameters:

- 1) Command Parameter: ***0 00 00 00 10 10 11***
 Partial Tag ID: *XX XX XX X0 10 11 XX XX*
- 2) Command Parameter: ***0 00 00 00 00 01 11 10***
 Partial Tag ID: *XX XX XX XX XX 11 10 XX*
- 3) Command Parameter: ***0 00 00 00 00 00 00 00 11***
 Partial Tag ID: *XX XX XX XX XX XX XX X1*
- 4) Command Parameter: ***1 01 10 11 00***
 Partial Tag ID: *01 10 11 00 XX XX XX*

Leading **0** don't care mask bits + **1** = mask header (not part of Partial Tag ID)

X = don't care mask bits

Table 7-26. Interrogator Command Parameters

Command	Parameter 1	Parameter 2
SelectGroup = <i>00 10 0</i>	Mask header: $\langle m-1 \rangle \times 0 + 1$	Partial Tag ID
5 bits	$\langle m \rangle$ bits, ($m = 1 \dots$ Tag ID length)	$\langle n \rangle$ bits, ($1 \dots$ Tag ID Tag ID length)

Table 7-27. Tag Response

SOF
Start of Frame
3 .. 10-bit period

7.14 SelectNGroup

When receiving the SelectNGroup command, all tags in the READY state which do not match the partial Tag ID will enter the Selected state and answer with the SOF pattern. The partial Tag ID can vary length. It's pattern position relative to the Tag ID is set by the first (leftmost) 1 in the command parameter. The preceding 0 bits act solely as "don't care" spacer bits. This "mask header" is not part of the actual partial Tag ID. The mask pattern follows the mask header and is terminated by the end of command.

Example of SelectNGroup Parameters:

Sample Tag ID 6CB9 : *01 10 11 00 10 11 10 01*

The above Tag ID would be selected by all the following GroupNSelect command parameters:

- 1) Command Parameter: *0 00 00 00 10 00 11*
 Partial Tag ID: *XX XX XX X0 00 11 XX XX*
- 2) Command Parameter: *0 00 00 00 00 01 11 11*
 Partial Tag ID: *XX XX XX XX XX 11 11 XX*
- 3) Command Parameter: *0 00 00 00 00 00 00 10*
 Partial Tag ID: *XX XX XX XX XX XX XX X0*
- 4) Command Parameter: *1 00 10 11 00 10 11 10 01*
 Partial Tag ID: *00 10 11 00 10 11 10 01*

Leading 0 don't care mask bits + 1 = mask header (not part of Partial Tag ID)

X = don't care mask bits

Table 7-28. Interrogator Command Parameters

Command	Parameter 1	Parameter 2
SelectGroup = <i>00 10 1</i>	Mask header: $\langle m-1 \rangle \times 0 + 1$	Matching pattern section of Tag ID
5 bits	$\langle m \rangle$ bits; $m = 1 \dots \text{Tag ID length} - 2$	$\langle n \rangle$ bits; $n = 2 \dots$

Table 7-29. Tag Response

SOF
Start of Frame
3 .. 10-bit period

7.15 ArmClear

A selected tag, when receiving the ArmClear command with the Master Key NOT set to 6 will prepare the device for a subsequent ClearAll command.

If this command is followed by any command other than a ClearAll, it will become disarmed. In which case the ArmClear must be repeated before a ClearAll can be successfully executed.

Table 7-30. Interrogator Command

Command	Parameter
ArmClear = <i>00 11 00 10 00</i>	<i>00 00 00</i>
10 bits	6 bits

Table 7-31. Tag Response

SOF
Start of Frame
3 .. 10-bit period

7.16 ClearAll

Tags in the Selected state, if previously armed by the ArmClear command will clear all memory blocks and their lock bits with the exception of the traceability data blocks (see [Figure 2-3 on page 4](#) in “Memory” section).

The ClearAll command includes an EEPROM programming sequence. The maximum EEPROM programming time is 6 ms. On completion of a successful clear the tag replies with a single SOF pattern.

If for any reason the clear operation fails, the tag will generate the corresponding error code. The error code bits are dual pattern coded (see [Figure 3-2 on page 11](#) and [Table 7-2 on page 26](#)) and are preceded by a SOF pattern. If the constant downlink checksum CRC_d (if appended) is incorrect, the clear operation is aborted and an error response is returned immediately.

Table 7-32. Interrogator Command Parameters

Command	Parameter 1	Parameter 2	Parameter 3	CRC (Optional)
ClearAll = <i>00 01</i>	<i>01 11 11</i>	<i>00</i>	32×0 bits	CRC_u = 96ADh
4 bits	6 bits	2 bits	32 bits	16 bits

Table 7-33. Tag Response

SOF	Error Flags
Start of Frame	Present on error only
3 .. 10-bit period	4-bit – dual pattern code

8. Absolute Maximum Ratings

Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Parameters	Symbol	Value	Unit
Maximum DC current into Coil 1/Coil 2	I_{coil}	20	mA
Maximum AC current into Coil 1/Coil 2 $f = 125$ kHz	$I_{coil p}$	20	mA
Power dissipation (dice) (free-air condition, time of application: 1 s)	P_{tot}	100	mW
Electrostatic discharge maximum to MIL–Standard 883 C method 3015	V_{max}	2000	V
Operating ambient temperature range	T_{amb}	–40 to +85	°C
Storage temperature range (data retention reduced)	T_{stg}	–40 to +150	°C

9. Electrical Characteristics

$T_{amb} = +25^{\circ}\text{C}$; $f_{coil} = 125$ kHz; unless otherwise specified

No.	Parameters	Test Conditions	Symbol	Min.	Typ.	Max.	Unit	Type*
1	RF frequency range		f_{RF}	100	125	250	kHz	
2.1	Supply current (without current consumed by the external LC tank circuit)	$T_{amb} = 25^{\circ}\text{C}^{(3)}$ (see Figure 9-1 on page 37)	I_{DD}		3	5	μA	T
2.2		Read – full temperature range			4	7	μA	Q
2.3		Program EEPROM				25	40	μA
3.1	Coil voltage (AC supply)	POR threshold (50 mV hysteresis)	$V_{coil pp}$	3.2	3.6	4.0	V	Q
3.2		Read, Select, Login command ⁽²⁾		6		V_{clamp}	V	Q
3.3		Write/program EEPROM ⁽²⁾		6		V_{clamp}	V	Q
4	Start-up time	$V_{coil pp} = 6$ V	$t_{startup}$		2.5	3	ms	Q
5	Clamp voltage	10 mA current into Coil 1/Coil 2	V_{clamp}	7		16	V	T
			V_{clamp}/T_{amb}		–7.5			Q
6.1	Modulation parameters	$V_{coil pp} = 6$ V on test circuit generator and modulation ON ⁽⁴⁾	$V_{mod pp}$		4.2	4.8	V	T
6.2			$I_{mod pp}$	400	600		μA	T
6.3			Thermal stability	V_{mod}/T_{amb}		–4.5		mV/°C

*) Type means: T: directly or indirectly tested during production; Q: guaranteed based on initial product qualification data

- Notes:
- EEPROM device performance can be influenced by subsequent customer assembly processes especially if subjected to high temperatures or mechanical stress conditions. So Atmel confirms these parameters only for devices as they leave the Atmel production, as undiced wafers or diced wafers in tray, etc.
 - Current into Coil 1/Coil 2 is limited to 10 mA. The damping characteristics are defined by the internally limited supply voltage (= minimum AC coil voltage).
 - I_{DD} measurement setup $R = 100$ k Ω ; $V_{CLK} = V_{coil} = 5$ V; EEPROM programmed to 00 ... 000 (erase all); NRZ, public mode.
 $I_{DD} = (V_{OUTmax} - V_{CLK})/R$
 - V_{mod} measurement setup: $R = 2.3$ k Ω ; $V_{CLK} = 3$ V; setup with modulation enabled (see [Figure 9-1 on page 37](#)).
 - The tolerance of the on-chip resonance capacitor is $\pm 10\%$ at 3 σ over whole production. The capacitor tolerance is $\pm 3\%$ at 3 σ on a wafer basis.

9. Electrical Characteristics (Continued)

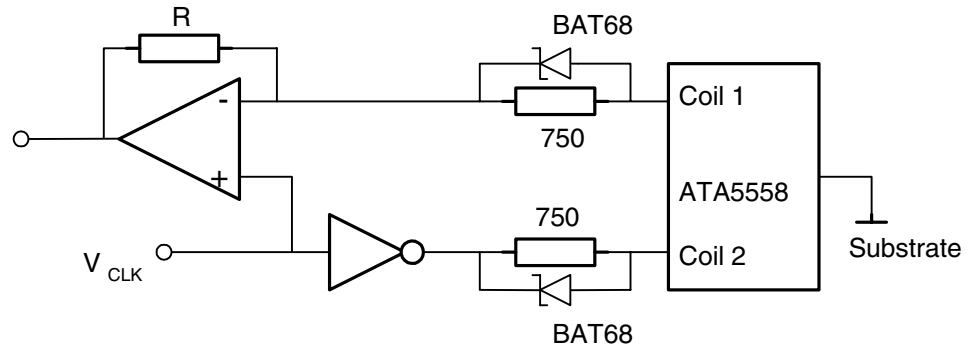
$T_{amb} = +25^{\circ}\text{C}$; $f_{coil} = 125\text{ kHz}$; unless otherwise specified

No.	Parameters	Test Conditions	Symbol	Min.	Typ.	Max.	Unit	Type*
7	Programming time	From last command gap to SOF pattern (36 + 648 internal clocks)	T_{prog}	5	5.7	6	ms	T
8	Endurance	Erase all/Write all ⁽¹⁾	n_{cycle}	100000			Cycles	Q
9.1	Data retention	$T_{op} = 55^{\circ}\text{C}$ ⁽¹⁾	$t_{retention}$	10	20	50	Years	
9.2		$T_{op} = 150^{\circ}\text{C}$ ⁽¹⁾	$t_{retention}$	96			hrs	T
9.3		$T_{op} = 250^{\circ}\text{C}$ ⁽¹⁾	$t_{retention}$	24			hrs	Q
10	Resonance capacitor	Mask option ⁽⁵⁾	Cr	70	78	86	pF	T

*) Type means: T: directly or indirectly tested during production; Q: guaranteed based on initial product qualification data

- Notes:
- EEPROM device performance can be influenced by subsequent customer assembly processes especially if subjected to high temperatures or mechanical stress conditions. So Atmel confirms these parameters only for devices as they leave the Atmel production, as undiced wafers or diced wafers in tray, etc.
 - Current into Coil 1/Coil 2 is limited to 10 mA. The damping characteristics are defined by the internally limited supply voltage (= minimum AC coil voltage).
 - I_{DD} measurement setup $R = 100\text{ k}\Omega$; $V_{CLK} = V_{coil} = 5\text{ V}$; EEPROM programmed to 00 ... 000 (erase all); NRZ, public mode. $I_{DD} = (V_{OUTmax} - V_{CLK})/R$
 - V_{mod} measurement setup: $R = 2.3\text{ k}\Omega$; $V_{CLK} = 3\text{ V}$; setup with modulation enabled (see [Figure 9-1 on page 37](#)).
 - The tolerance of the on-chip resonance capacitor is $\pm 10\%$ at 3s over whole production. The capacitor tolerance is $\pm 3\%$ at 3σ on a wafer basis.

Figure 9-1. Measurement Setup for V_{mod}



10. Ordering Information⁽¹⁾

ATA5558	a b	M c c	- x x x Package	Drawing
			- DDW - Dice on wafer, 6" un-sawn wafer, thickness 300 µm - DDT - Dice in Tray (waffle pack), thickness 300 µm (-PAE - NOA-2 Micromodule planned) (-PP - Plastic Transponder planned)	See Figure 10-2 on page 40 See Figure 10-3 on page 41
			Customer ID ⁽²⁾	
			M01 - Atmel standard (corresponds to 00) - Customer X unique ID code ⁽¹⁾	
			11 - 2 pads without on-chip C	See Figure 10-1 on page 39
			12 - 2 pads with on-chip 80 pF	See Figure 10-1 on page 39
			14 - 2 pads with on-chip 210 pF	See Figure 10-1 on page 39
			(15 - Micromodule with 330 pF planned)	See Figure 10-1 on page 39

- Notes:
- For available order codes refer to Atmel Sales/Marketing
 - Unique customer ID code programming according to [Figure 2-3 on page 4](#) is linked to a minimum order quantity of 1 Mio parts per year

10.1 Delivery Pre-configuration

The ATA5558 is delivered in a pre-programmed state. The traceability blocks (59-61) contain unique non erasable traceability data as described in section "[Traceability Data](#)" on page 5. The remaining memory contains erasable demonstration data which can be replaced by customer data after having been cleared using a sequence of Select, ArmClear and ClearAll commands. the demonstration data represents the following device configuration:

Block 63 contains configuration data representing Public Mode, FDX-B Modulation, a data rate of RF/32, a Tag ID length of 64 bits, preamble value of 7 and a maximum public mode block value (Maxblock) of 3.

Blocks 0-3 contain an FDX-B encoded animal ID code in accordance with ISO 11784 representing a National ID code 000123456789 and country code 999.

The Tag ID blocks 56-57 contain a direct copy of the unique traceability data held in blocks 59-60 thus each delivered device will have it's own 64 bit unique Tag ID code with which anticollision arbitration can be demonstrated.

All other blocks are erased.

10.2 Ordering Examples (Recommended)

ATA555811 - Tested dice on unsawn 6" wafer, thickness 300 µm, no on-chip capacitor, no damping during POR initialization.

10.3 Package Information

Figure 10-1. 2 Pad Layout for Wire Bonding

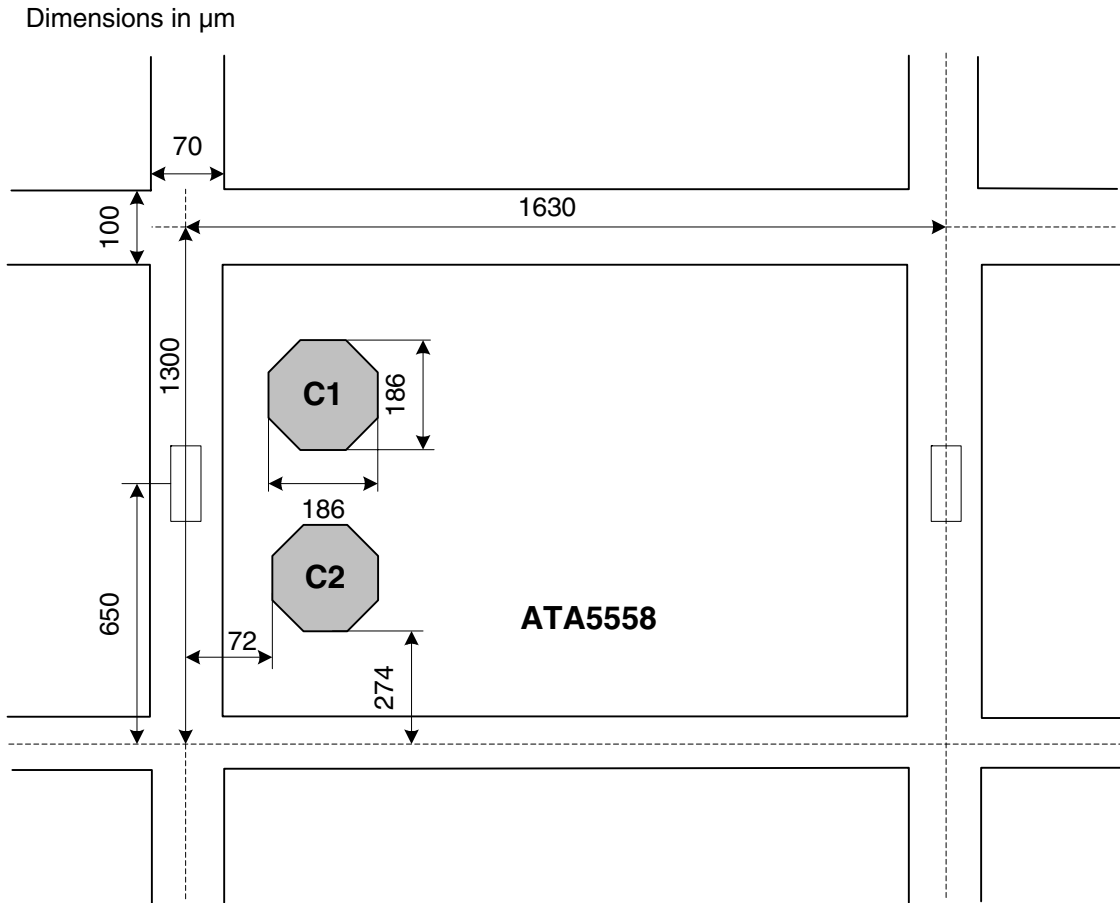
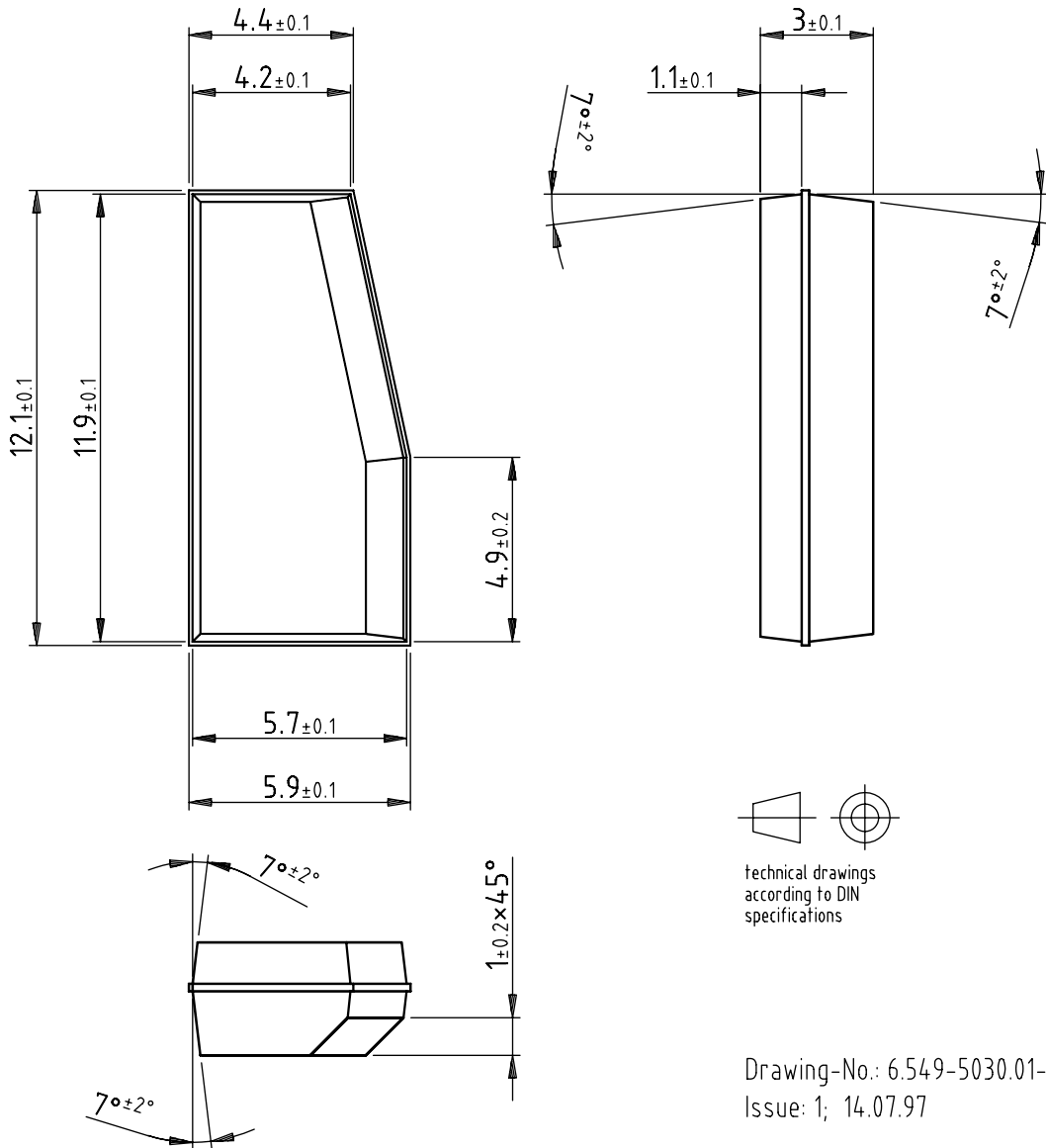


Figure 10-3. Plastic Transponder

Package: Transponder
 Dimensions in mm



Drawing-No: 6.549-5030.01-4
 Issue: 1; 14.07.97



Atmel Corporation

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

Regional Headquarters

Europe

Atmel Sarl
Route des Arsenaux 41
Case Postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia

Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

Japan

9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Atmel Operations

Memory

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

Microcontrollers

2325 Orchard Parkway
San Jose, CA 95131, USA
Tel: 1(408) 441-0311
Fax: 1(408) 436-4314

La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
Tel: (33) 2-40-18-18-18
Fax: (33) 2-40-18-19-60

ASIC/ASSP/Smart Cards

Zone Industrielle
13106 Rousset Cedex, France
Tel: (33) 4-42-53-60-00
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park
Maxwell Building
East Kilbride G75 0QR, Scotland
Tel: (44) 1355-803-000
Fax: (44) 1355-242-743

RF/Automotive

Theresienstrasse 2
Postfach 3535
74025 Heilbronn, Germany
Tel: (49) 71-31-67-0
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906, USA
Tel: 1(719) 576-3300
Fax: 1(719) 540-1759

Biometrics/Imaging/Hi-Rel MPU/ High Speed Converters/RF Datacom

Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
Tel: (33) 4-76-58-30-00
Fax: (33) 4-76-58-34-80

Literature Requests

www.atmel.com/literature

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© Atmel Corporation 2005. All rights reserved. Atmel®, logo and combinations thereof, Everywhere You Are®, IDIC® and others, are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.



Printed on recycled paper.

4681C-RFID-09/05