Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

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: 80 pF ±12%, 210 pF ±12% 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

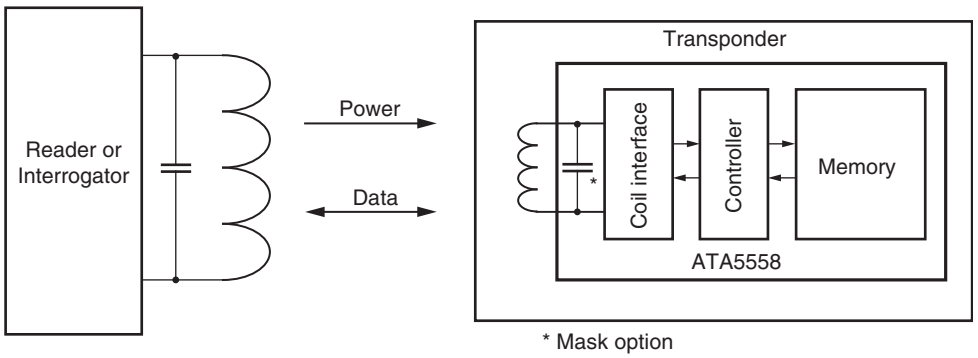
1 kbit R/W IDIC with Deterministic Anticollision

ATA5558

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

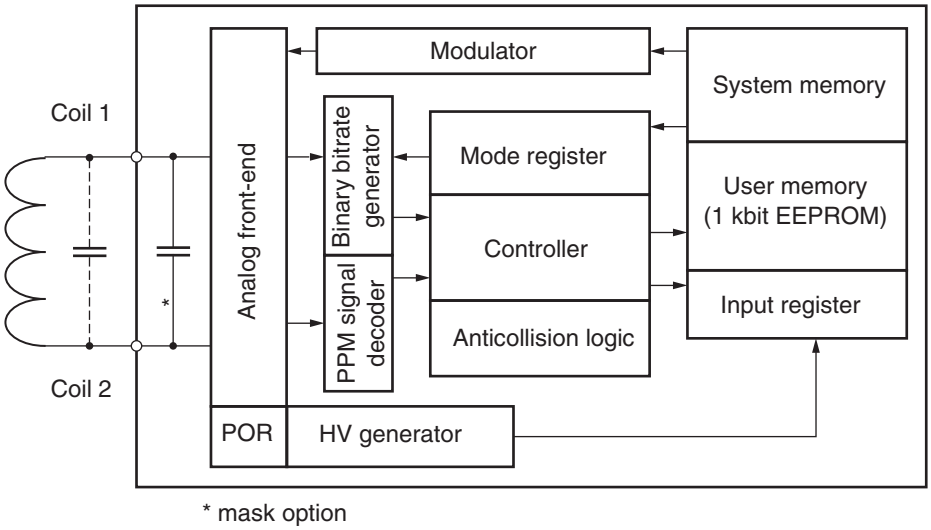


It contains an EEPROM which is subdivided into 1024 bits of user memory and 320 bits of system memory. Both memory sections are organized in data blocks of 32 bits, each equipped with an associated lock bit for block write protection. The user memory, which is intended for storage of recallable user 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.

4681E–RFID–11/09

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	*0* = modulation off *1* = 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

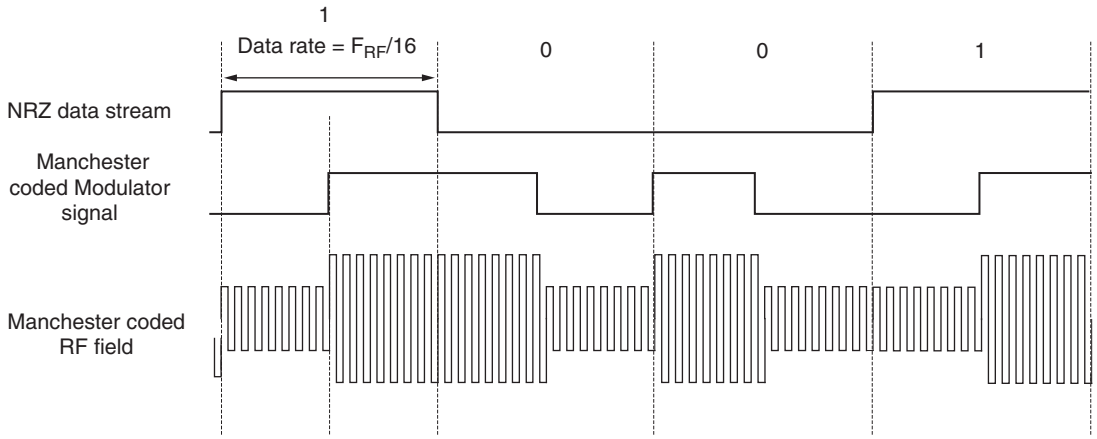
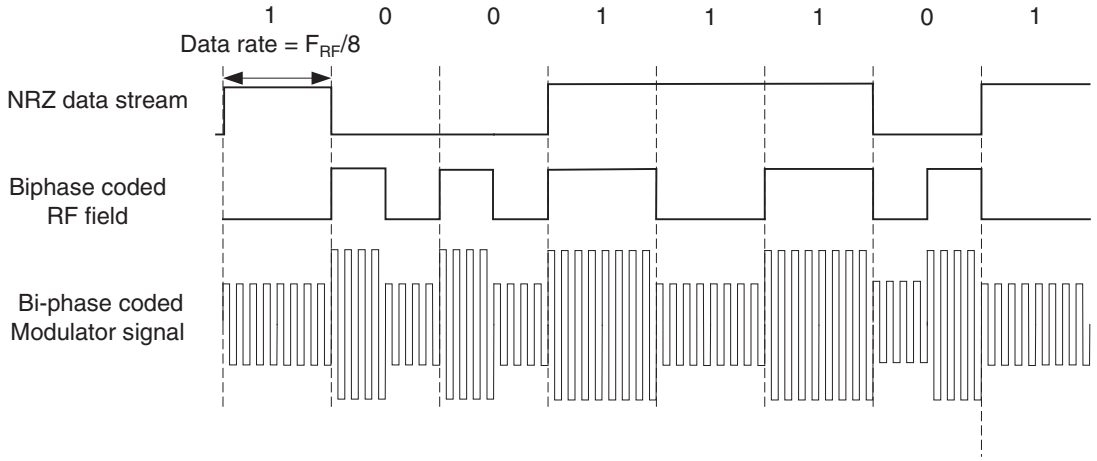


Figure 2-2. Bi-phase Timing Diagram



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.

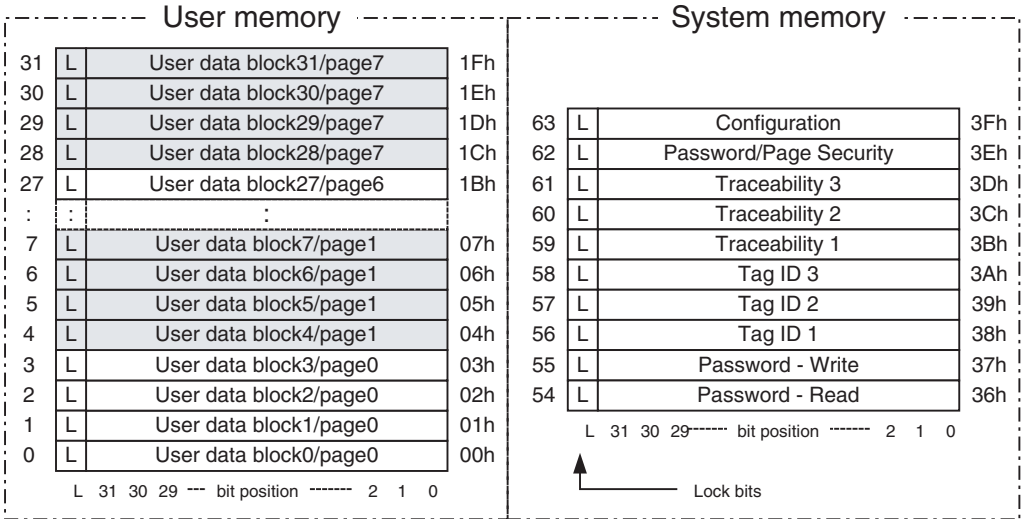
$$\text{Data rate} = \frac{RF}{2(n+1)}$$

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).

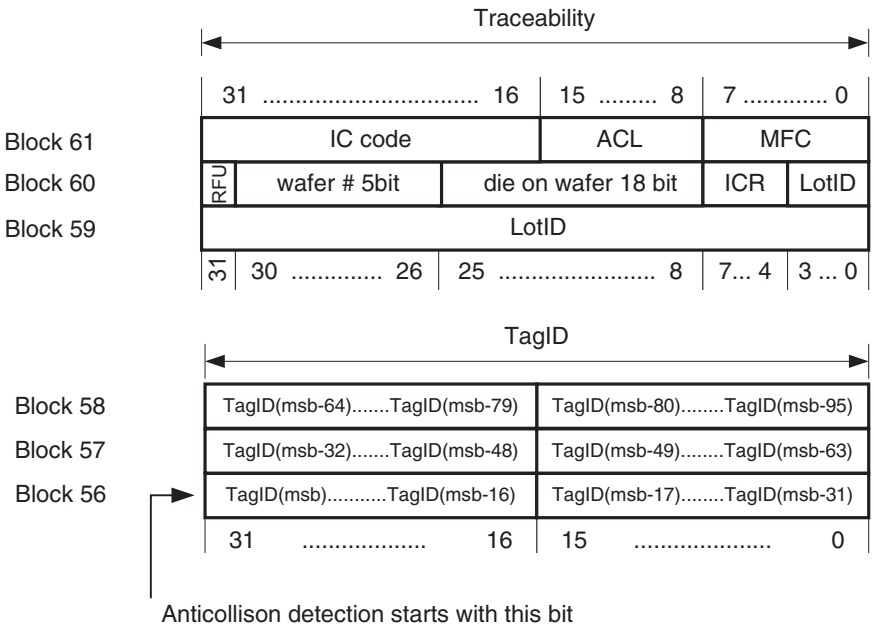
All the configuration settings are allocated in block 63 (see Figure 2-7 on page 9) and the password protection security information in block 62 (see Figure 2-6 on page 7).

2.6.2 Traceability Data

The traceability information is programmed and locked into the traceability blocks (59-61) by Atmel during the production test(1).

Note: 1. This is not valid for -DDW (tested die on unsawn wafer) delivery.

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 number 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 specifiy 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 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

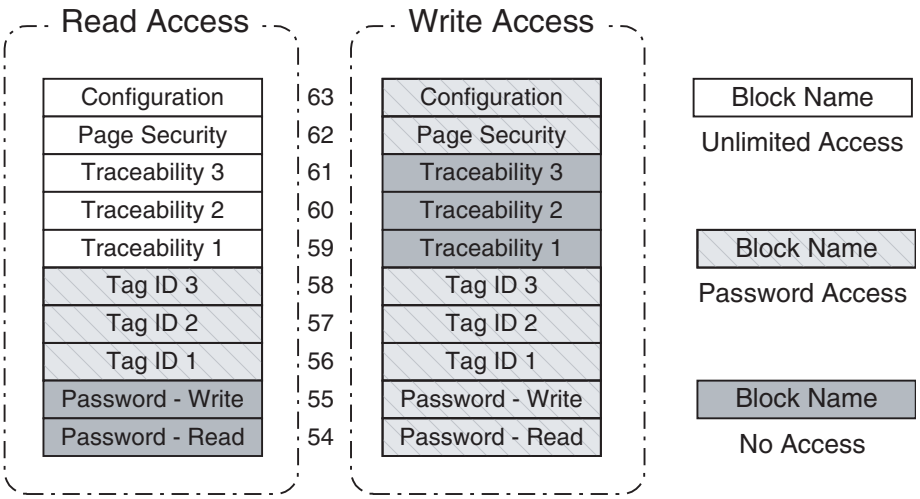
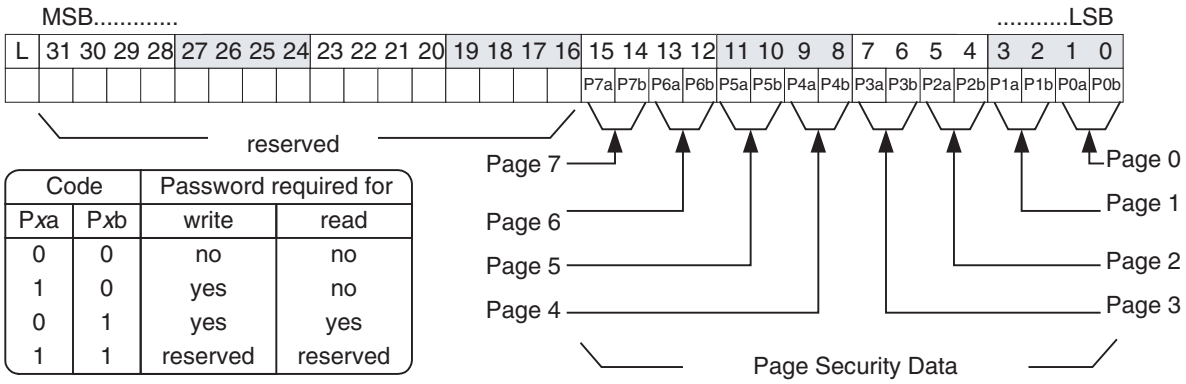


Figure 2-6. Page Security Register



Code		Password required for	
P*x*a	P*x*b	write	read
0	0	no	no
1	0	yes	no
0	1	yes	yes
1	1	reserved	reserved

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

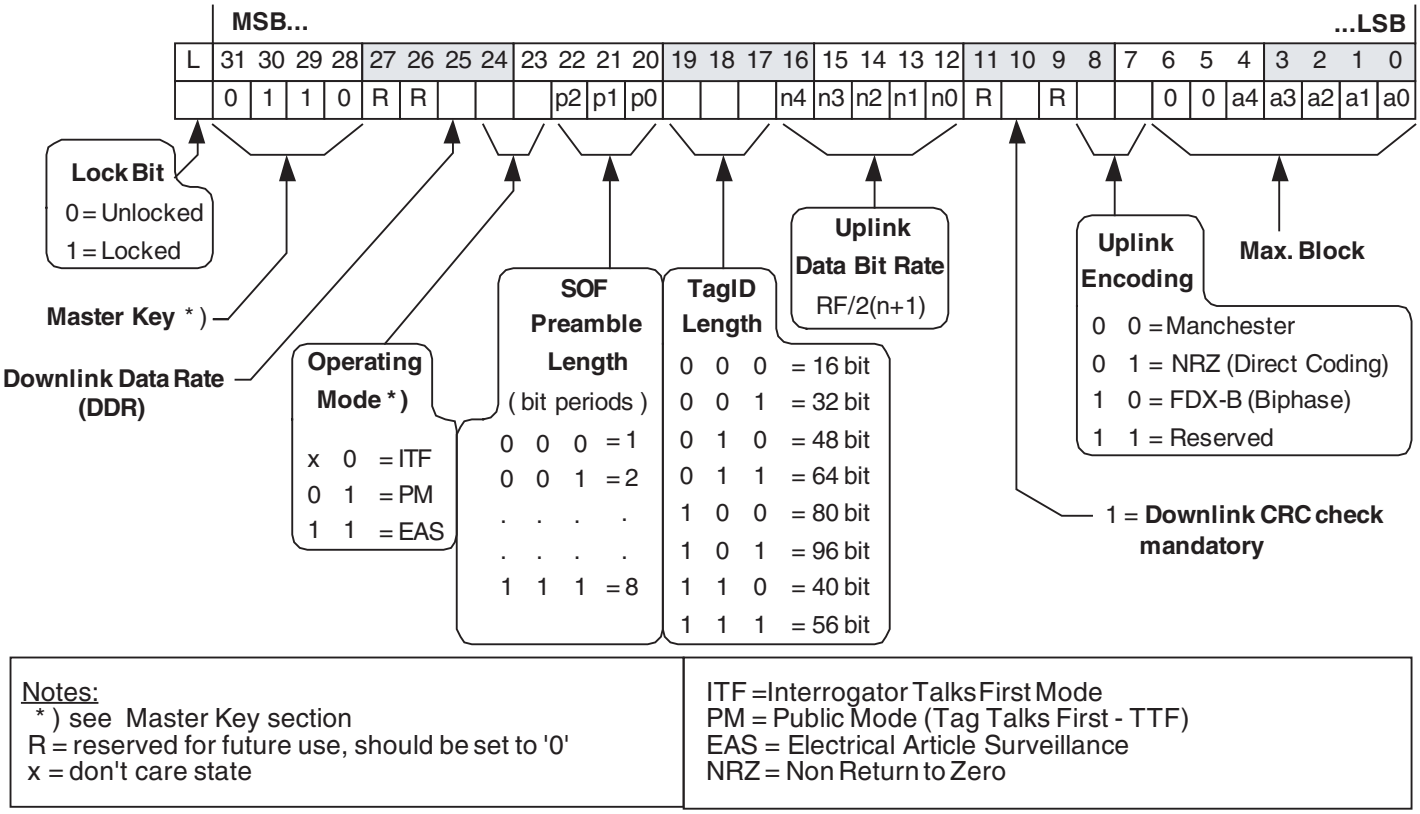
	Enables				Protection Scheme	
Master Key	**DDR**	**PM**	**EAS**	**User Memory Clear**	**Page Security**	**System Memory**
6	yes	yes	yes	no	yes	yes
9	yes	yes	yes	yes	yes	yes
others	no	no	no	yes	no	no

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:
*) see Master Key section
R = reserved for future use, should be set to '0'
x = don't care state

ITF = Interrogator Talks First Mode
PM = Public Mode (Tag Talks First - TTF)
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)

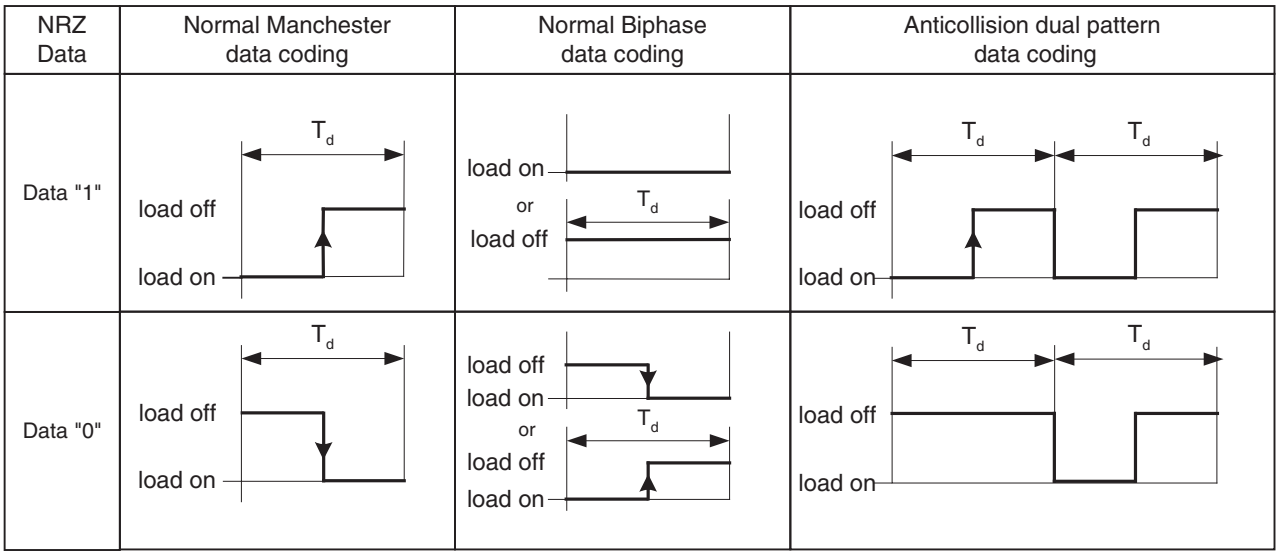
3.1 Tag to Interrogator Communication

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

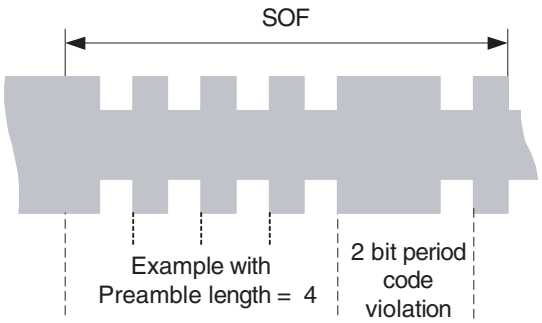
Figure 3-1. Tag to Interrogator - Load Modulation Coding



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



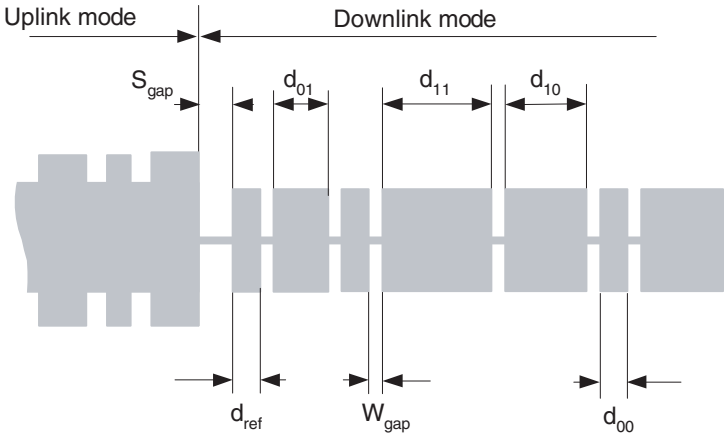
3.1.2 Public Mode

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 restarted. Commands or partial command sequences occurring during the power on reset sequence will not 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 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 $T_C = 1/f_C = 8$ µs ($f_C = 125$ 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 vary slightly.

Figure 3-4. Command “Read Block #23”

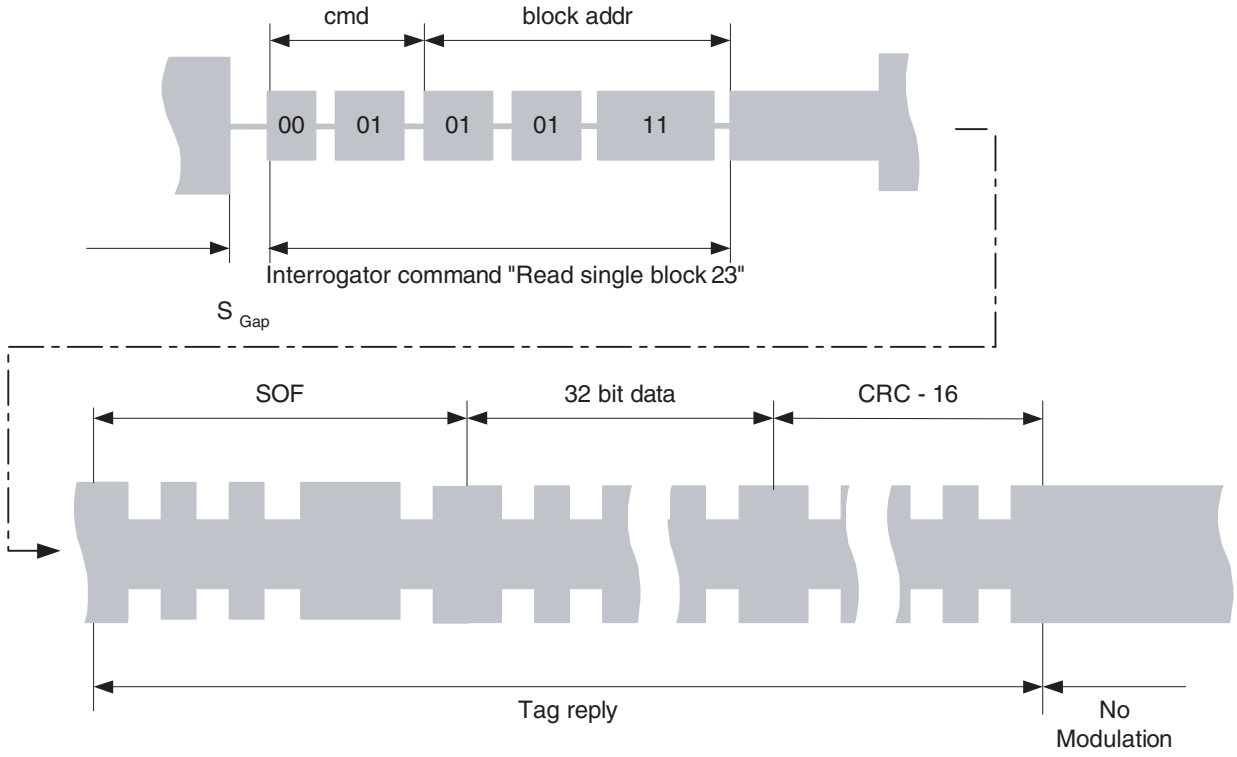
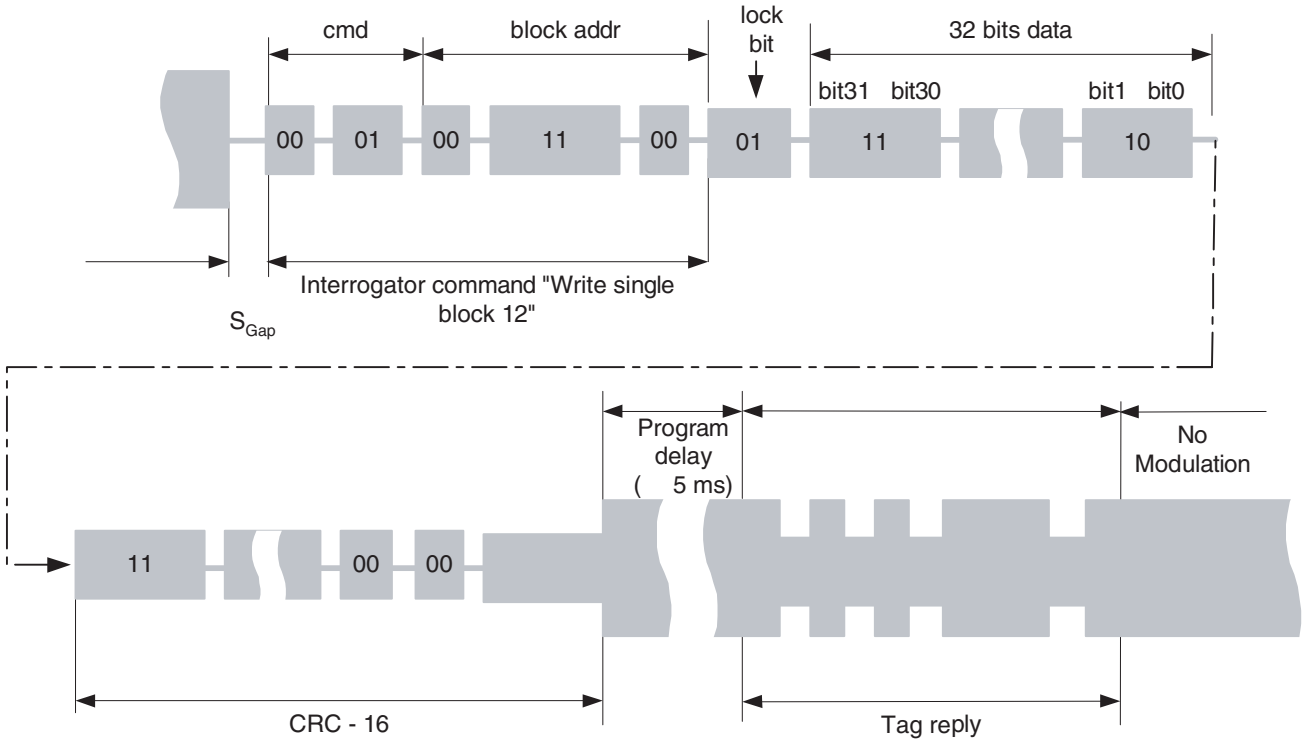


Figure 3-5. Command “Write Block #12”



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

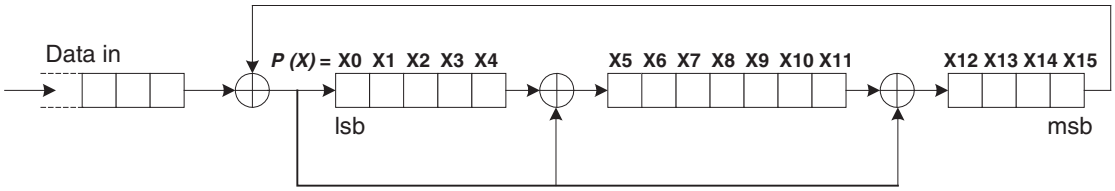


Figure 4-2. Examples of Downlink CRC Generation

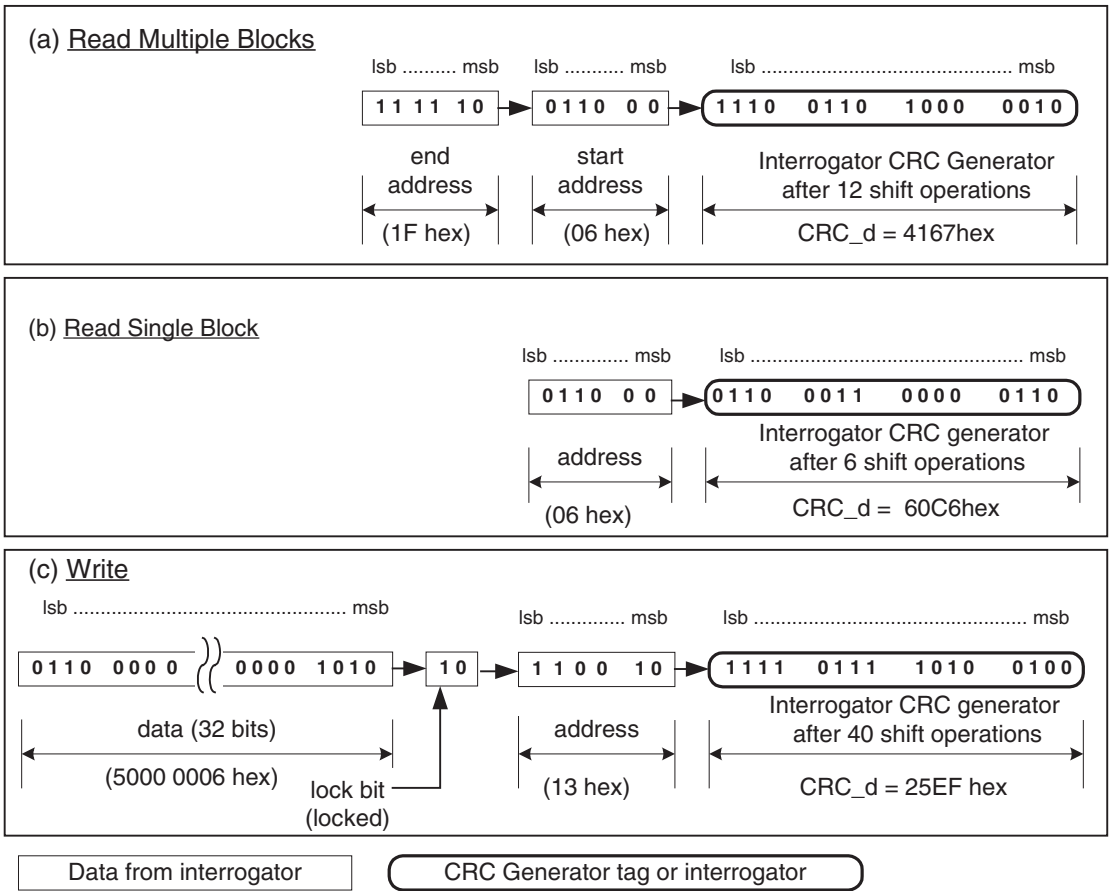
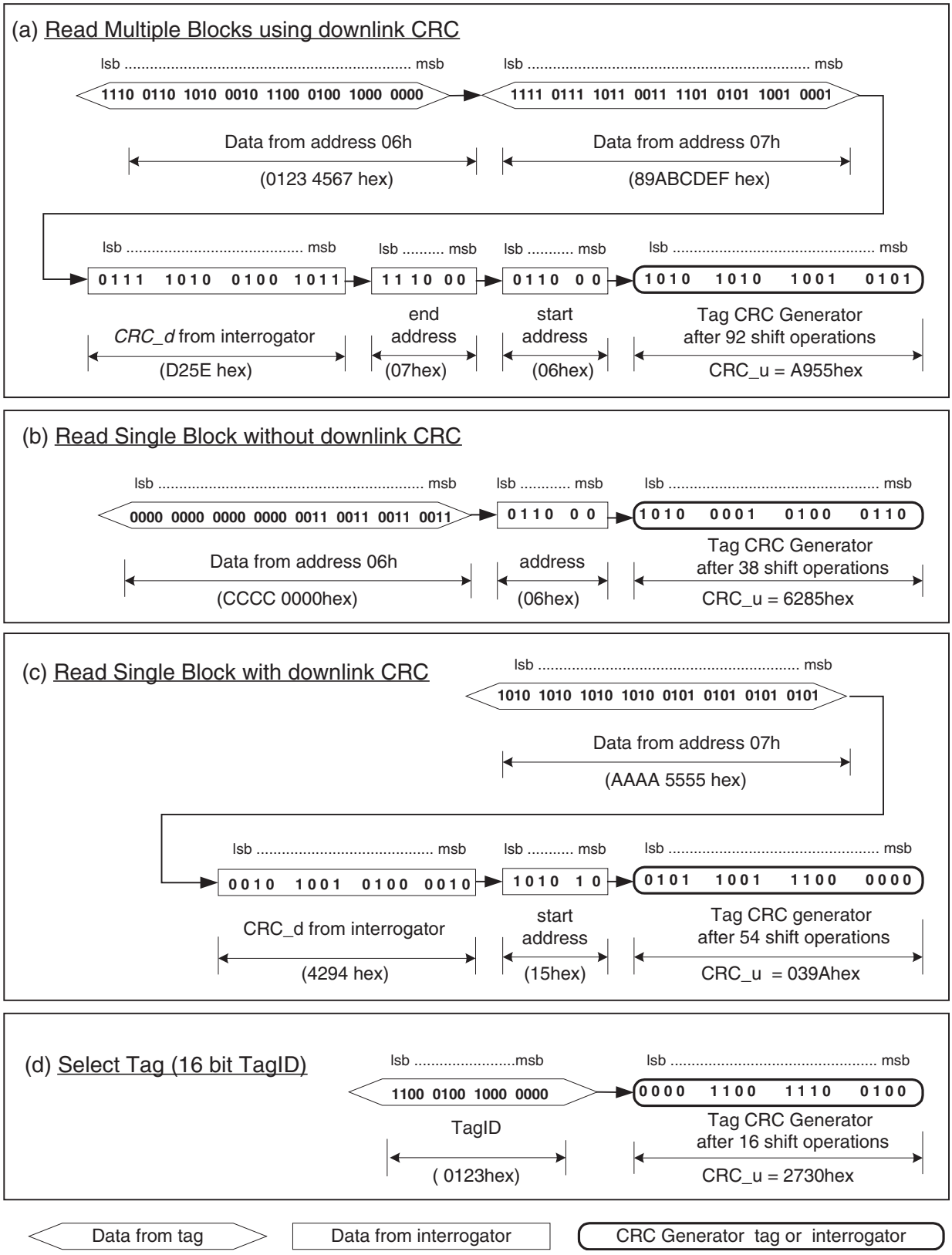


Figure 4-3. Examples of Uplink CRC Generation



5. Operating Modes

After initialization, the Operating Mode (Configuration block bits 23 and 24) is interrogated and depending on it's 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.

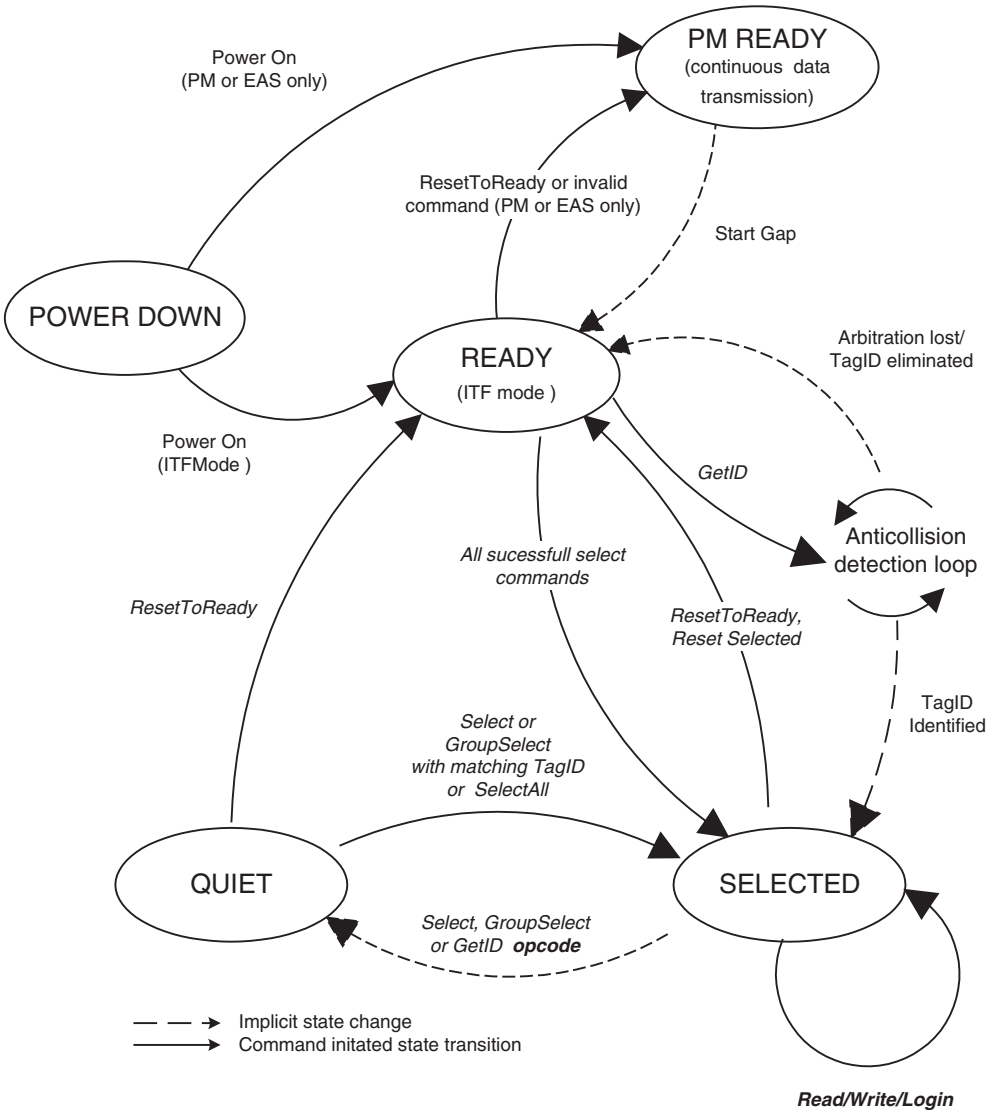
5.5 Selected State

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

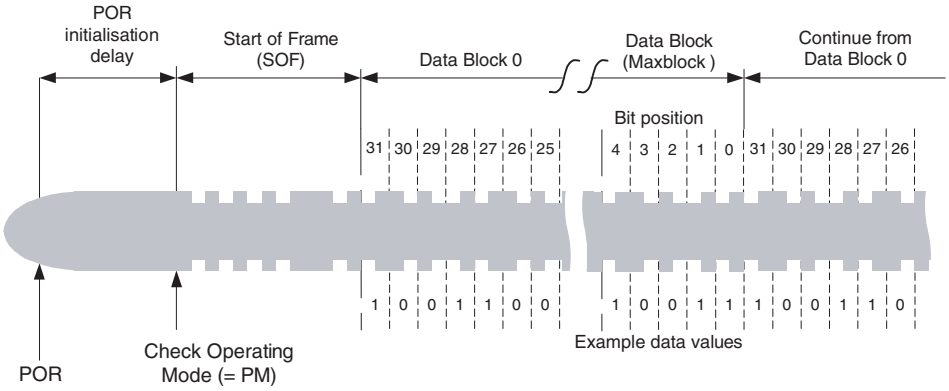
The tag goes into the Quiet state from the Selected state when a new selection takes place i.e. a Select or a GetID command is received. Unlike the READY state, the tag's Tag ID in this state is known. Tags in the Quiet state are excluded from subsequent anticollision detection.

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.

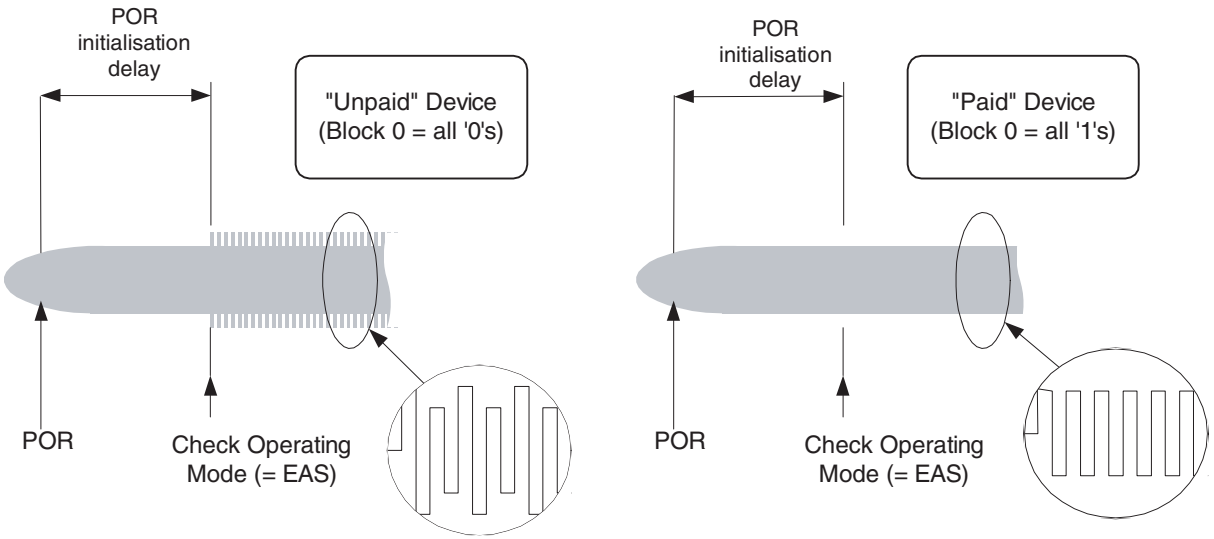
Figure 5-2. Public Mode Start Up



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 it's 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 it's 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

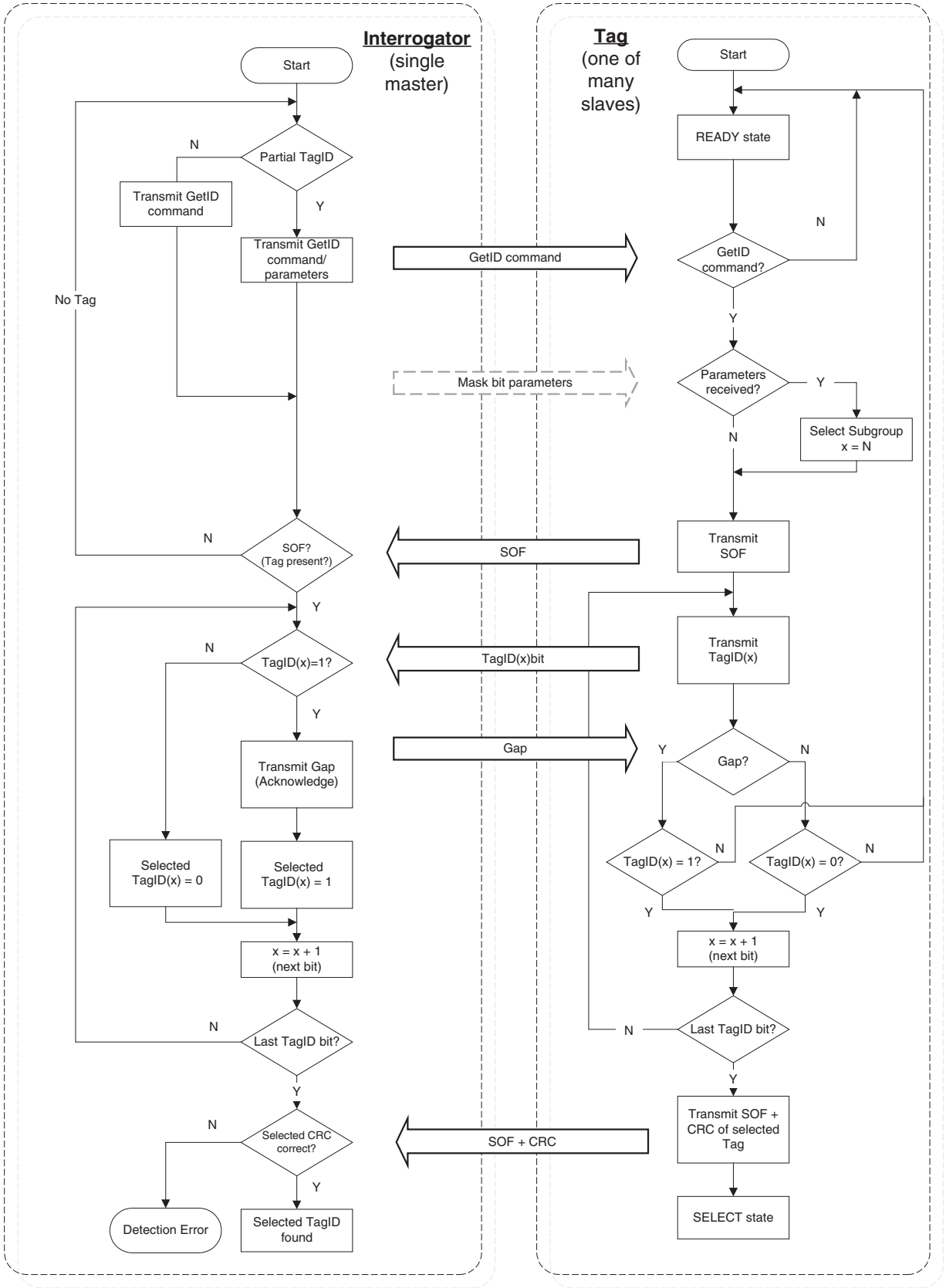


Figure 6-2. GetID Command with Partially Known Tag ID

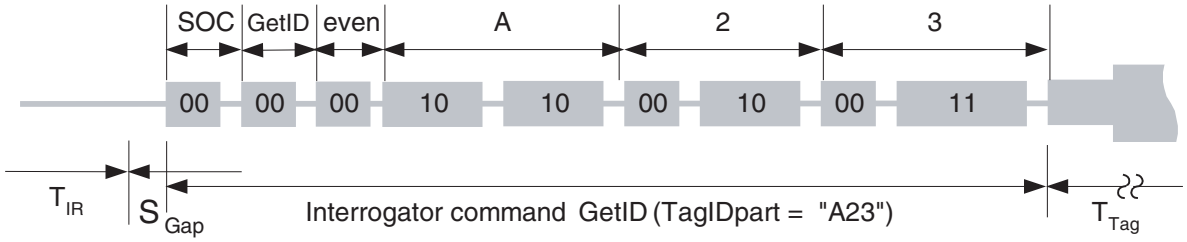


Figure 6-3. Subsequent Tag Responses in Anticollision Loop (Two Alternative Tag IDs)

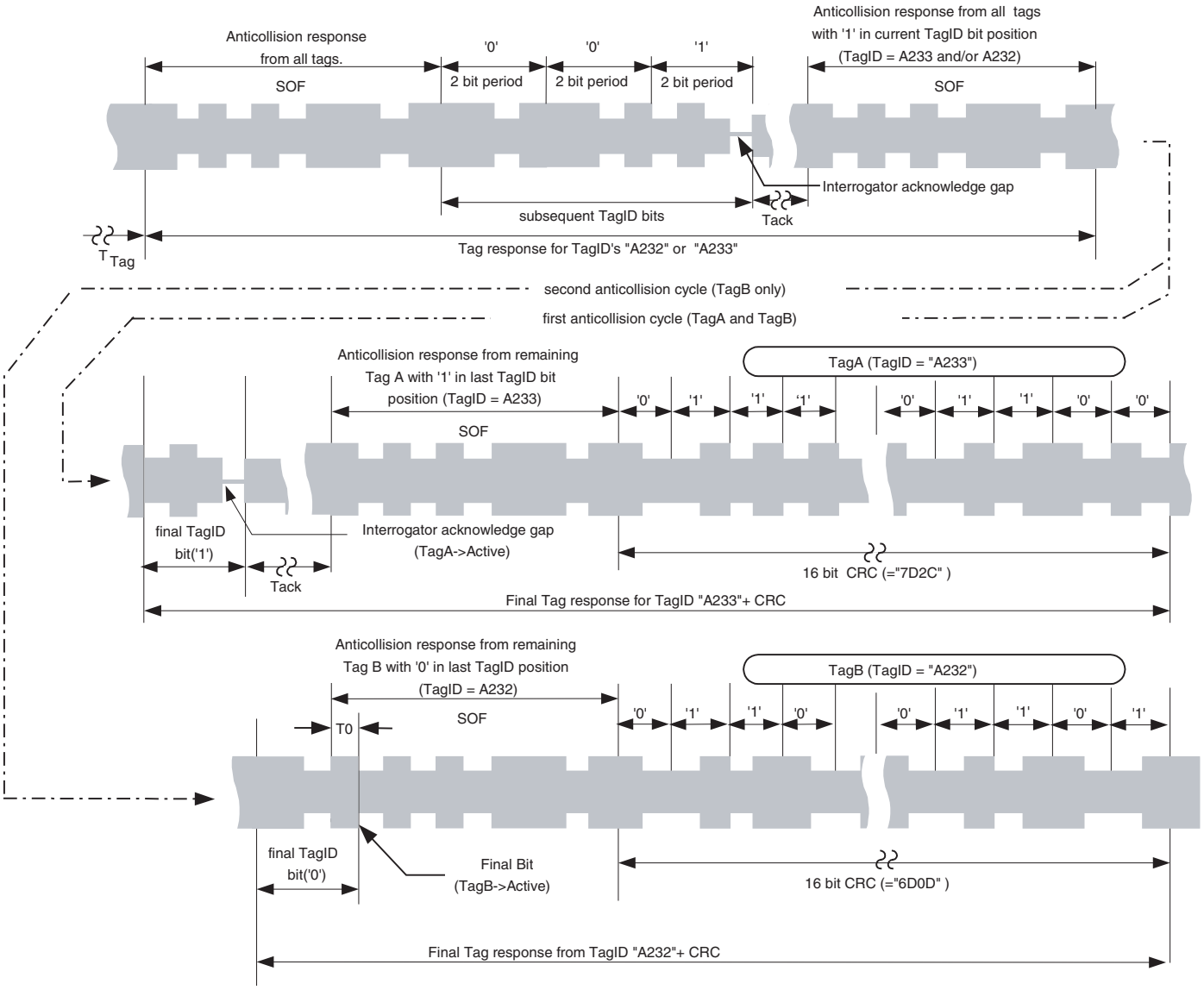


Table 6-1. Anti-collision Timing

Parameter	Remark	Symbol	Formular	Formular	Example: $T_{bit} = 32 / f_c$, $d_{ref} = 24 \times T_c$	
Tag reaction time	End of start gap to start of tag command processing	T_{IR}			$\geq 0 \times T_c$	
Tag to Interrogator response time	End of final command gap to start of Tag SOF	T_{Tag}	d_{11} max + $65 \times T_c$ (See Table 3-1 on page 12)		DDR = 1	$117 \times T_c$
					DDR = 0	$145 \times T_c$
Anticollision Aknowledge response time	End of Interrogator acknowledge gap to start of Tag SOF	T_{ack}	DDR = 1	$134 \times T_c$	$134 \times T_c$	
			DDR = 0	$138 \times T_c$	$138 \times T_c$	
Anticollision final zero bit response time	Overlap of final zero bit and SOF	T_0	$½ \times T_{bit}$	$½ \times T_{bit}$	$16 \times T_c$	

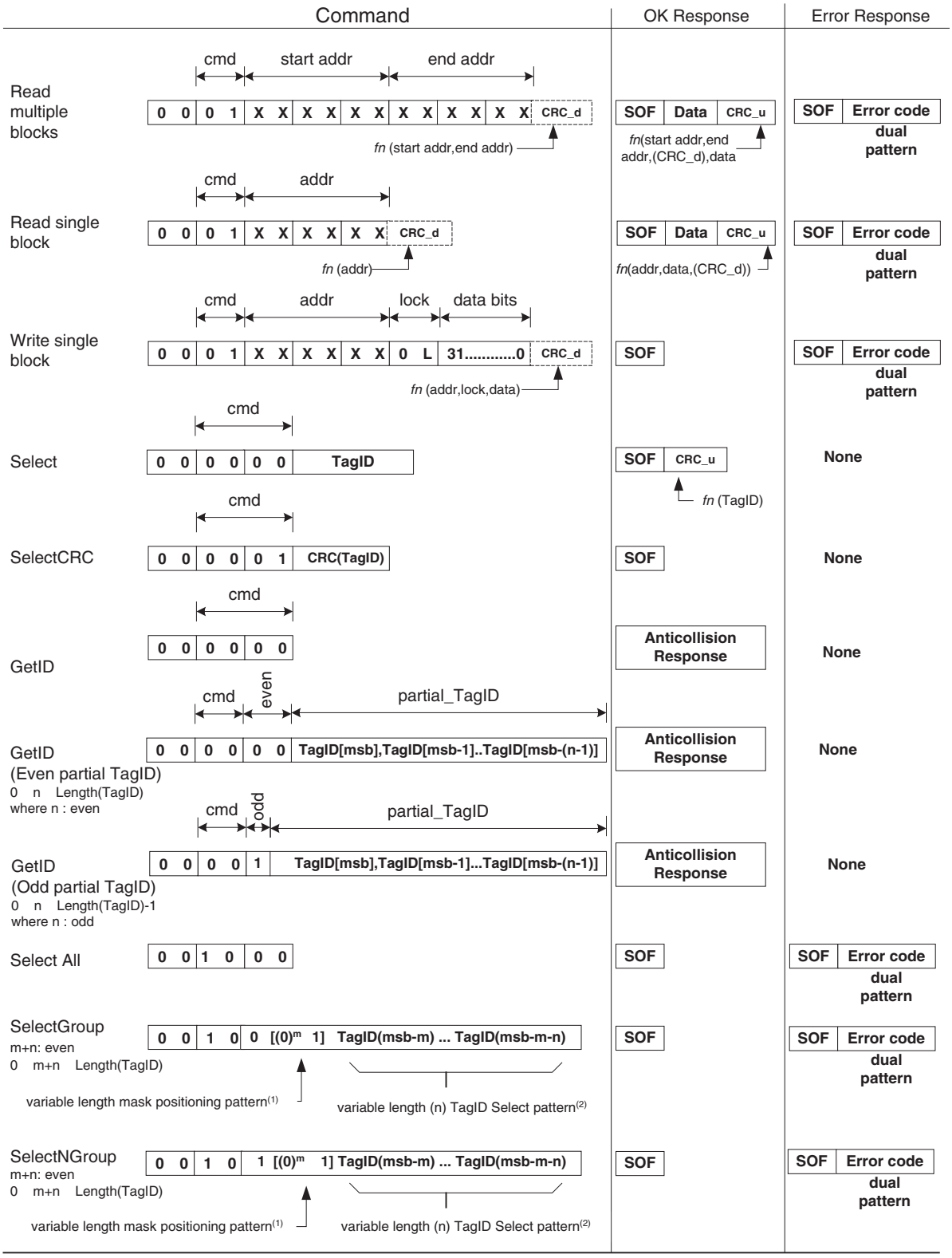
7. Command Set

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.