Chip Card & Security ICs FT4452

Intelligent 256-Byte EEPROM with Write and Read-Out Protect Function and Programmable Security Code (PSC)

FEATURES

- Low voltage and low power operations:
  - FT4452: V_{CC} = 2.5V to 5.5V
  - FT4452A: V_{CC} = 1.8V to 5.5V
- 256×8 bit EEPROM organization of Data Memory
- 32×1 bit organization of Protection Memory.
- Byte-wise addressing.
- Byte-wise write protection of first 32 address of Data Memory
- Read-out protection of Data Memory and Protection Memory before verification of 3 Bytes PSC
- Data Memory alterable only after verification of 3 Bytes PSC
- End of processing indicated at data output
- PSC verification trials limited by Error Counter
- Contact configuration and Answer-to-Reset (synchronous transmission) in accordance to standard ISO/IEC 7816
- EEPROM erase/write time 5ms.
- ESD protection typical 4,000 V.
- Minimum of 100,000 erase/write cycles.
- Data retention for minimum of ten years.

1. DESCRIPTION

FT4452 is contact configuration memory card chip. The devices are fabricated with proprietary advanced CMOS process for low power and low voltage applications. A standard 2-wire serial interface is used to address all read and write functions. Our extended V_{CC} range (1.8V to 5.5V) devices enables wide spectrum of applications.

1.1 Pin Description

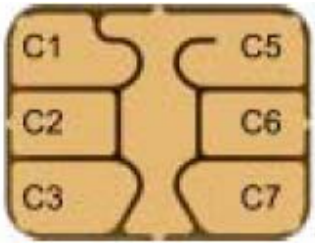


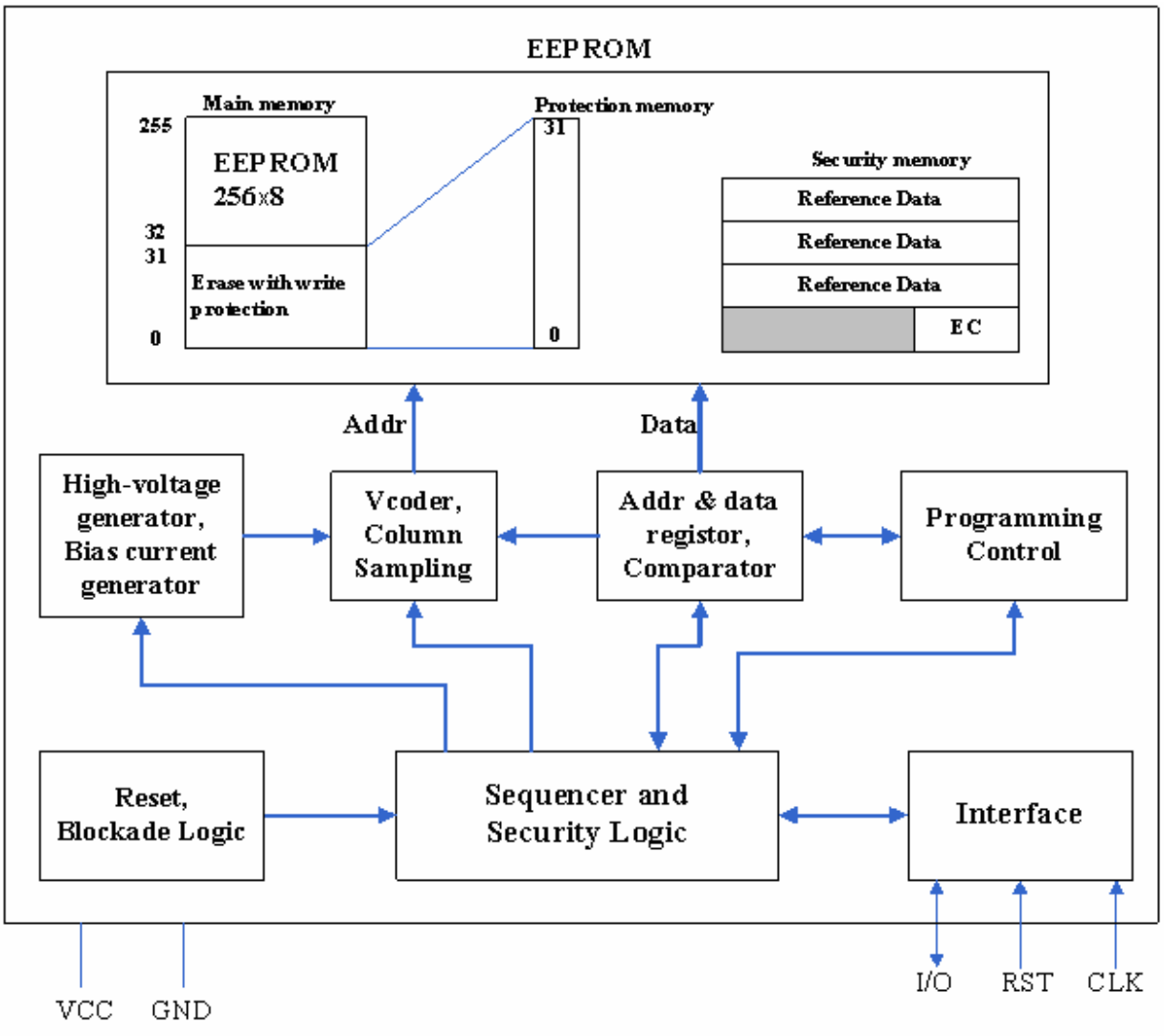
Figure1 Pin Configuration Wire-bonded Module M3.2 (top view)

1.2 Pin Definitions and Functions

Card contact	Symbol	Function
C1	VCC	Supply voltage
C2	RST	Control input(Reset Signal)
C3	CLK	Clock input
C5	GND	Ground
C6	N.C.	Not connected
C7	I/O	Bi-directional data line(open drain)

2. FUNCTION DISCRIPTION

Block Diagram



2.1 Circuit Description

Erase/Write Operation

The FT4452 consists of 256 x 8 bit EEPROM main memory and a 256-bit protection memory with PROM functionality. The main memory is erased and written byte by byte. When erased, all 8 bits of a data byte are set to logical one. When written, the information in the individual EEPROM cells is, according to the input data, altered bit by bit to logical zeros (logical AND between the old and the new data in the EEPROM). Normally a data change consists of an erase and write procedure. It depends on the contents of the data byte in the main memory and the new data byte whether the EEPROM is really erased and/or written. If none of the 8 bits in the addressed byte requires a zero to-one transition the erase access will be suppressed. Vice versa the write access will be suppressed if no one-to-zero transition is necessary. The write and the erase operation takes at least 2.5 ms each.

Write Protection of Data Memory

Each of the first 32 bytes can be irreversibly protected against data change by writing the corresponding bit in the protection memory. Each data byte in this address range is assigned to one bit of the protection memory and has the same address as the data byte in the main memory which it is assigned to. Once written the protection bit cannot be erased (PROM).

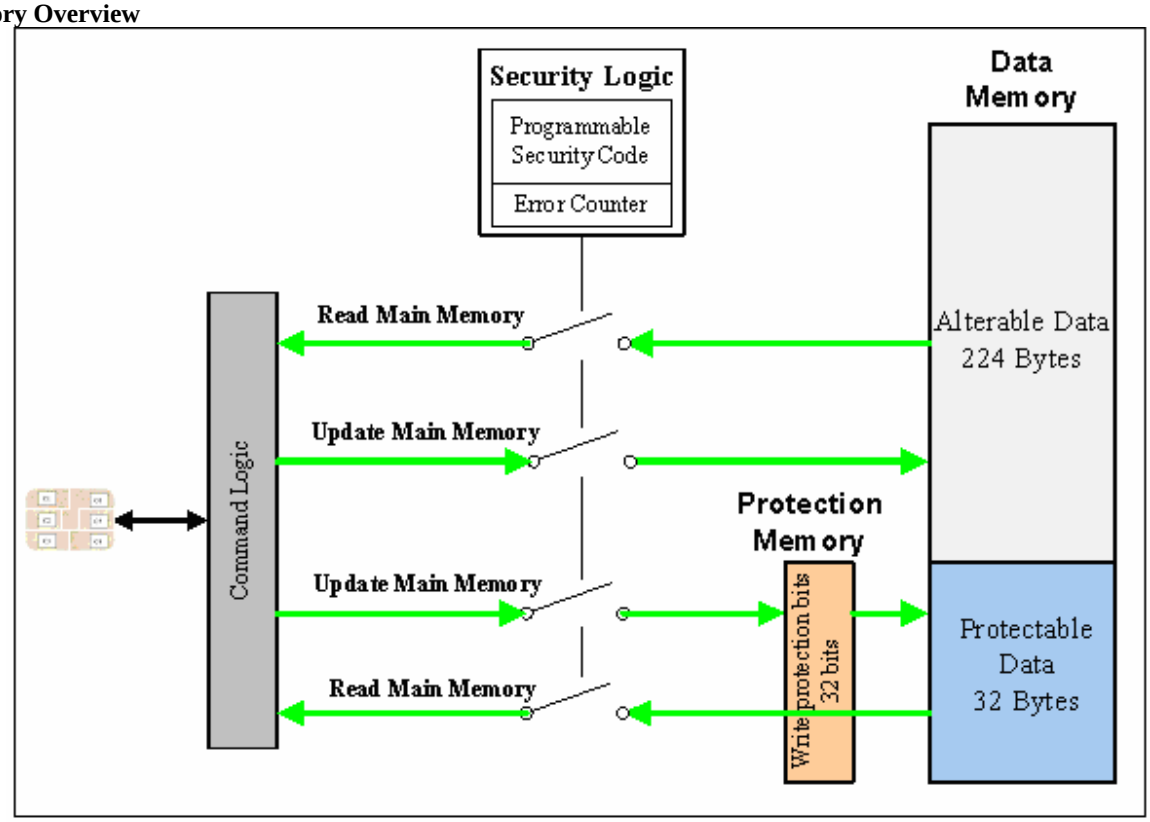
Read-Out Protection of Data Memory and Protection Memory

Data Memory and Protection Memory readable only after verification of 3-Byte Programmable Security Code (PSC)

Programmable Security Code

FT4452 provides a security code logic which controls the write/erase access to the memory. For this purpose the FT4452 contains a 4-byte security memory with an Error Counter EC (bit 0 to bit 2) and 3 bytes reference data. These 3 bytes as a whole are called Programmable Security Code (PSC). After power on the whole memory, except for the Error Counter, can not be read or write. Only after a successful comparison of verification data with the internal reference data the read/write access to memory is active until the power is switched off. After three successive unsuccessful comparisons the Error Counter blocks any subsequent attempt, and hence any possibility to write and erase.

Memory Overview



2.2 Transmission Protocol

The transmission protocol is a two wire link protocol between the interface device IFD and the integrated circuit IC. It is identical to the protocol type "S = A". All data changes on I/O are initiated by the falling edge on CLK.

The transmission protocol consists of the 4 modes:

- Reset and Answer-to-Reset
- Command Mode
- Outgoing Data Mode
- Processing Mode

Note: The I/O pin is open drain and therefore requires an external pull up resistor to achieve a high level.

2.2.1 Reset and Answer-to-Reset

Answer-to-Reset takes place according to ISO standard 7816-3 (ATR). The reset can be given at any time during operation. In the beginning, the address counter is set to zero together with a clock pulse and the first data bit (LSB) is output to I/O when RST is set from level H to level L. Under a continuous input of additional 31 clock pulses the contents of the first 4 EEPROM addresses is read out. The 33rd clock pulse switches I/O to high impedance Z and finishes the ATR procedure.

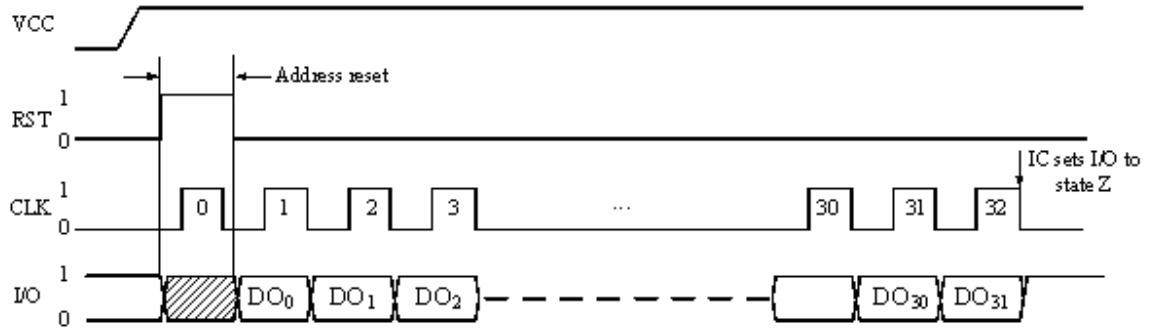


Figure 2 Reset and Answer-to-Reset

2.2.2 Operational Modes

Command Mode
After the Answer-to-Reset the chip waits for a command. Every command begins with a start condition, includes a 3 bytes long command entry followed by an additional clock pulse and ends with a stop condition.

- Start condition: Falling edge on I/O during CLK in level H
- Stop condition: Rising edge on I/O during CLK in level H

After the reception of a command there are two possible modes:

- Outgoing data mode for reading
- Processing mode for writing and erasing

Outgoing Data Mode
In this mode the IC sends data to the IFD. The first bit becomes valid on I/O after the first falling edge on CLK. After the last data bit an additional clock pulse is necessary in order to set I/O to high impedance Z and to prepare the IC for a new command entry. During this mode any start and stop condition is discarded.

Processing Mode
In this mode the IC processes internally. The IC has to be clocked continuously until I/O, which was switched to level L after the first falling edge of CLK, is set to high impedance level Z. Any start and stop condition is discarded during this mode.

Note: The RST line is low during the modes mentioned above. If RST is set to high during the CLK low level any operation is aborted and I/O is switched to high impedance Z (Break).

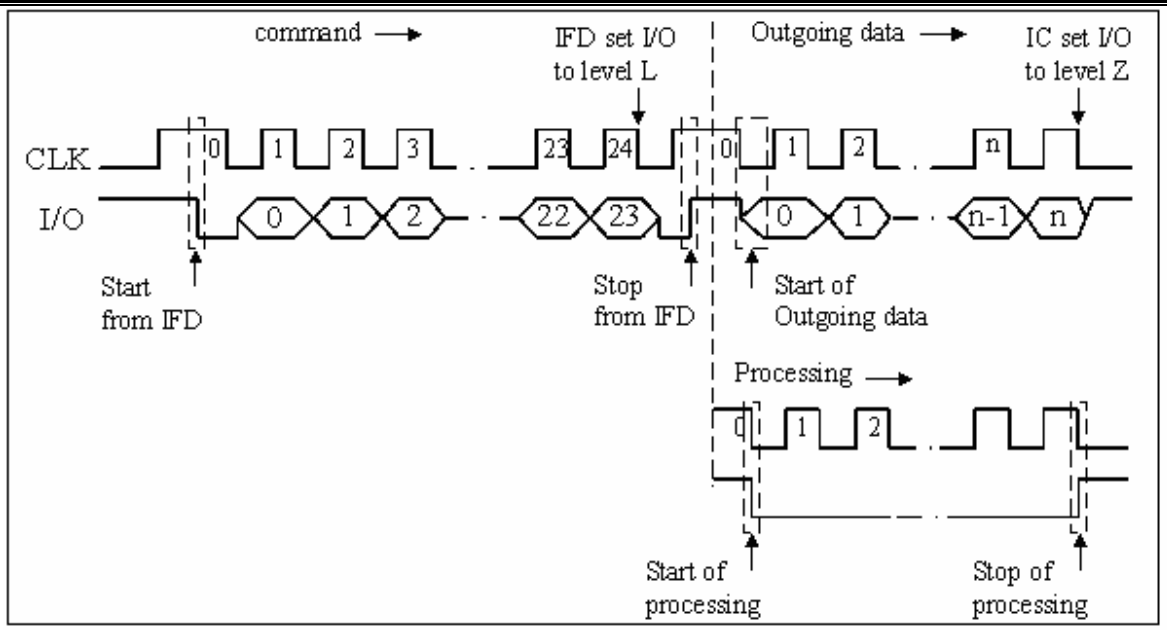


Figure 3 Operational Modes

2.3 Commands

Command Format

Each command consists of three bytes:

MSB Control LSB								MSB Address LSB								MSB Data LSB							
B7	B6	B5	B4	B3	B2	B1	B0	A7	A6	A5	A4	A3	A2	A1	A0	D7	D6	D5	D4	D3	D2	D1	D0

Beginning with the control byte LSB is transmitted first.

The FT4452 provides 7 commands which are listed in **table 1**.

Table1

Byte1 Control								Byte2 Address	Byte3 Data	Operation	Mode
B7	B6	B5	B4	B3	B2	B1	B0	A7-A0	D7-D0		
0	0	1	1	0	0	0	0	address	No effect	READ MAIN MEMORY	Outgoing data
0	0	1	1	1	0	0	0	address	Input data	UPDATE MAIN MEMORY	processing
0	0	1	1	0	1	0	0	No effect	No effect	READ PROTECTION MEMORY	Outgoing data
0	0	1	1	1	1	0	0	address	Input data	WRITE PROTECTION MEMORY	processing
0	0	1	1	0	0	0	1	No effect	No effect	READ SECURITY MEMORY	Outgoing data
0	0	1	1	1	0	0	1	address	Input data	UPDATE SECURITY MEMORY	processing
0	0	1	1	0	0	1	1	address	Input data	COMPARE VERIFIVATION DATA	processing

2.3.1 Read Main Memory

The command reads out the contents of the main memory (with LSB first) starting at the given byte address (N = 0…255) up to the end of the memory. After the command entry the IFD has to supply sufficient clock pulses. The number of clocks

is m = (256 – N) × 8 + 1. The read access to the main memory is always possible.

2.3.2 Read Protection Memory

The command transfers the protection bits under a continuous input of 32 clock pulses to the output. I/O is switched to high impedance Z by an additional pulse. The protection memory can always be read, and indicates the data bytes of the main memory protected against changing.

2.3.3 Update Main Memory

The command programs the addressed EEPROM byte with the data byte transmitted. Depending on the old and new data, one of the following sequences will take place during the processing mode:

- erase and write (5 ms) corresponding to m = 255 clock pulses
- write without erase (2.5 ms) corresponding to m = 124 clock pulses
- erase without write (2.5 ms) corresponding to m = 124 clock pulses

(All values at 50 kHz clock rate.)

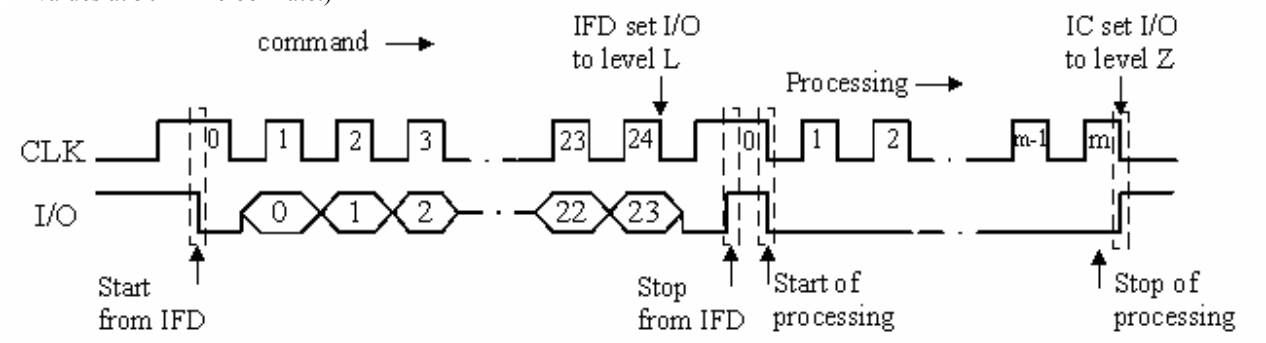


Figure 4 Read Main Memory

2.3.4 Write Protection Memory

The execution of this command contains a comparison of the entered data byte with the assigned byte in the EEPROM. In case of identity the protection bit is written thus making the data information unchangeable. If the data comparison results in data differences writing of the protection bit will be suppressed. Execution times and required clock pulses see UPDATE MAIN MEMORY.

2.3.5 Read Security Memory

Similar to the read command for the protection memory this command reads out the 4 bytes of the security memory. The number of clock pulses during the outgoing data mode is 32. I/O is switched to high impedance Z by an additional pulse. Without a preceding successful verification of the PSC the output of the reference bytes is suppressed, that means I/O outputs state L for the reference data bytes.

2.3.6 Update Security Memory

Regarding the reference data bytes this command will only be executed if a PSC has been successfully verified before. Otherwise only each bit of the error counter (Address 0) can be written from “1” to “0”. The execution times and the required clock pulses are the same as described under UPDATE MAIN MEMORY.

2.3.7 Compare Verification Data

This command can only be executed in combination with an update procedure of the error counter (see PSC verification). The command compares one byte of the entered verification data byte with the corresponding reference data byte. For this procedure clock pulses are necessary during the processing mode.

2.4 PSC Verification

The FT4452 requires a correct verification of the Programmable Security Code PSC stored in the Security Memory for altering data if desired.

The following procedure has to be carried out exactly as described. Any variation leads to a failure, so that a write/erase access will not be achieved. As long as the procedure has not been successfully concluded the error counter bits can only be

changed from “1” to “0” but not erased.

At first an error counter bit has to be written to “0” by an UPDATE command (**see figure 5**) followed by three COMPARE VERIFICATION DATA commands beginning with byte 1 of the reference data. A successful conclusion of the whole procedure can be recognized by being able to erase the error counter which is not automatically erased. Now write/erase access to all memory areas is possible as long as the operating voltage is applied. In case of error the whole procedure can be repeated as long as erased counter bits are available. Having been enabled, the reference data are allowed to be altered like any other information in the EEPROM.

The following table gives an overview of the necessary commands for the PSC verification. The sequence of the shaded commands is mandatory.

Command	Control	Address	Data	Remark
	B7…B0	A7…A0	D7…D0	
Read security Memory	31_H	No effect	No effect	Check Error Counter
Update Security Memory	39_H	00_H	Input data	Write free bit in Error Counter input data:0000 0ddd binary
Compare Verification Data	33_H	01_H	Input data	Reference Data Byte1
Compare Verification Data	33_H	02_H	Input data	Reference Data Byte2
Compare Verification Data	33_H	03_H	Input data	Reference Data Byte3
Update Security Memory	39_H	00_H	FF_H	Erase Error Counter
Read Security Memory	31_H	No effect	No effect	Check Error Counter

As shipped, the PSC is programmed with a code according to individual agreement with the customer. Thus, knowledge of this code is indispensable to alter data.

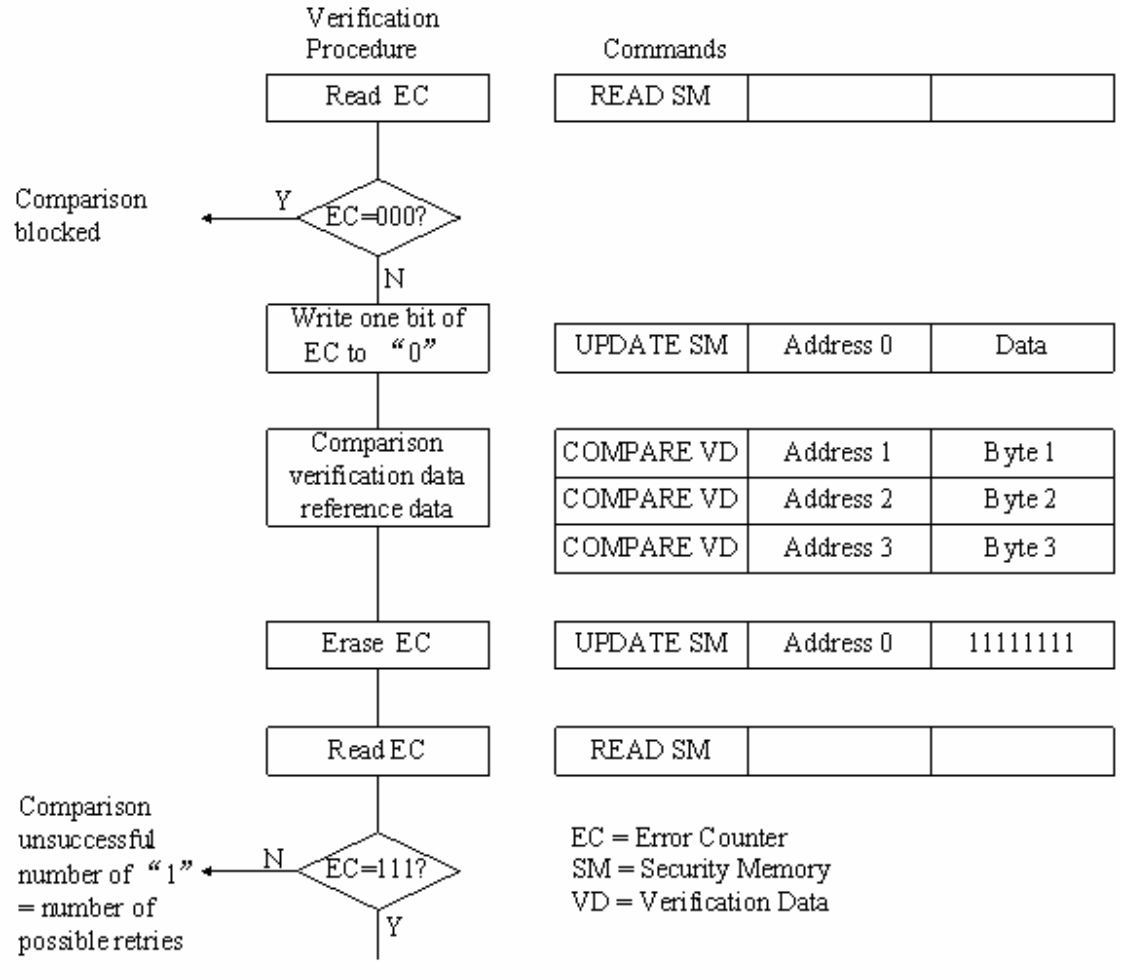


Figure 5 Verification Procedure

2.5 Reset Modes

Reset and Answer-to-Reset (compare 2.2.1)

Power on Reset

After connecting the operating voltage to VCC, I/O is high impedance Z. By all means, a read access to any address or an Answer-to-Reset must be carried out before data can be altered.

2.6 Break

If RST is set to high during CLK in state L any operation is aborted and I/O is switched to high impedance Z. Minimum duration of t_{RES} = 5 us is necessary to trigger a defined valid reset. After Break the chip is ready for further operations.

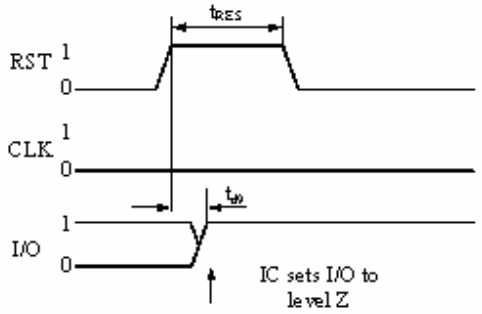


Figure 6 Break

2.7 Failures

Behavior in case of failures:
In case of one of the following failures, the chip sets the I/O to high impedance Z after 8 clock pulses at the latest.
Possible failures:

- Comparison unsuccessful
- Wrong command
- Wrong number of command clock pulses
- Write/erase access to already protected bytes
- Rewriting and erasing of a bit in the protection memory

3. OPERATIONAL INFORMATION

3.1 Memory Map

Address (decimal)	Main Memory	Protection Memory	Security Memory
255	Data Byte 255(D7…D0)		
. . .	. . .		
32	Data Byte 32(D7…D0)		
31	Data Byte 31(D7…D0)	Protection Bit 31(D31)	
. . .	. . .	. . .	
3	Data Byte 3(D7…D0)	Protection Bit 3(D3)	Reference Data Byte 3(D7…D0)
2	Data Byte 2(D7…D0)	Protection Bit 2 (D2)	Reference Data Byte 2(D7…D0)
1	Data Byte 1(D7…D0)	Protection Bit 1(D1)	Reference Data Byte 1(D7…D0)
0	Data Byte 0(D7…D0)	Protection Bit 0(D0)	Error Counter(0,0,0,0,0,D2,D1,D0)

The Data bytes 0 to 31 can be protected against further changes by programming the associated protection bit 0 to 31. The FT4452 allows data changing or reading only after correct verification of the Reference Data bytes. Otherwise Error Counter is the only memory access to read or write.

3.2 Electrical Characteristics

3.2.1 Absolute Maximum Ratings

Parameter	Symbol	Limit Values		Unit
		Min.	Max.	
Supply voltage	V_{CC}	-0.3	6.0	V
Input voltage(any pin)	V_1	-0.3	6.0	V
Storage temperature	T_{stg}	-40	125	℃
Power dissipation	P_{tot}		70	mW

Note: Stresses above 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 above those indicated in the operational sections of this data sheet is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability, including EEPROM data retention and write/erase endurance.

In the operating range the functions given in the circuit description are fulfilled.

3.2.2 Operation Range

Parameter	Symbol	Limit Values			Unit	Test Condition
		Min.	Typ.	Max.		
Supply voltage	V_{CC}	4.75	5.0	5.25	V	-
Supply current	I_{CC}		3	10	mA	V_{CC}=5V
Ambient temperature	T_A	0		70	℃	-

3.2.3 DC Characteristics

Parameter	Symbol	Limit Values			Unit	Test Condition
		Min.	Typ.	Max.		
High level input voltage (I/O,CLK,RST)	V_{IH}	3.5		V_{CC}	V	-
Low level input voltage (I/O,CLK,RST)	V_{IL}	0		0.8	V	-
High level input current (I/O,CLK,RST)	I_{IH}			50	μA	V_{IH}=5V
Low level output current (I/O)	I_{OL}	1			mA	V_{OL}=0.4V,open drain
High level output current (I/O)	I_{OH}			50	μA	V_{OH}=5V,open drain
Input capacitance	C_1			10	pF	

3.2.4 AC Characteristics

The AC characteristics refer to the timing diagrams in the following. V_{IHmin} and V_{ILmax} are reference levels for measuring timing of signals.

Parameter	Symbol	Limit Values			Unit	Test Condition
		Min.	Typ.	Max.		
CLK Frequence	CLK	7		50	KHz	-
CLK High time	t_H	9		0.8	μs	-
CLK Low time	t_L	9			μs	
CLK Rise time	t_R			1	μs	
CLK Fise time	t_F			1	μs	
I/O Low to CLK Hold time (Start Condition)	t_{d1}	4			μs	
RST Low to I/O Valid time	t_{d2}			2.5	μs	
CLK High to I/O clear time	t_{d3}	4			μs	
CLK Low to RST Hold time	t_{d4}	4			μs	
CLK Low to I/O Hold time	t_{d5}	1			μs	
RST High time (address reset)	t_{d6}	20			μs	
I/O Setup to CLK High time	t_{d7}	1			μs	
CLK High to I/O Hold time		4			μs	
Reset time for break	t_{RES}	5			μs	
RST High to I/O Clear time (break)		2.5				
Erase time	t_{ER}	2.5			ms	f_{CLK} = 50KHz
Write time		2.5			ms	f_{CLK} = 50KHz
I/O High time	t_{BUF}	10			μs	