# ST16CF54

## DATA SHEET

DS.CF54/9601V1

# ST16CF54

## REFERENCES

# TABLE OF CONTENTS









# LIST OF TABLES

## LIST OF FIGURES







SGS-THOMSON MICROELECTRONICS

# ST16CF54

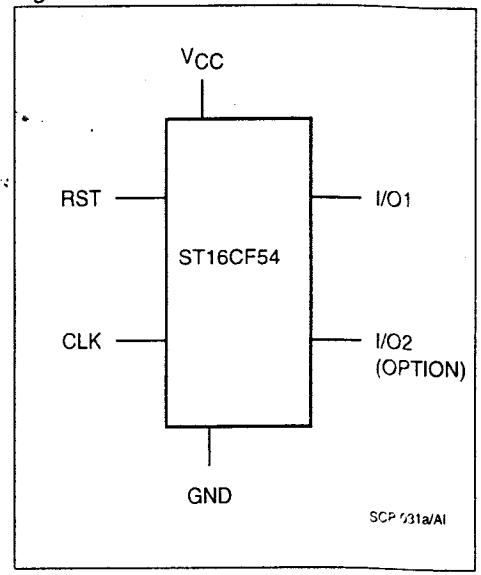
## CMOS MCU BASED SAFEGUARDED SMART CARD IC WITH MODULAR ARITHMETIC PROCESSOR

- 8 BIT ARCHITECTURE CPU
- 16 Kbytes OF USER ROM, SECTOR COMBINATIVE
- 4 Kbytes OF SYSTEM ROM
- 480 bytes OF RAM
- 4 Kbytes OF EEPROM, SECTOR COMBINATIVE
  - Highly reliable CMOS EEPROM technology
  - 10 years data retention
  - 100 000 Erase/Write cycles endurance
  - Protected One Time Programmable block (32 or 64 bytes)
  - Separate Write and Erase cycle for fast "1" programming
  - 1 to 32 bytes block Erase or Write in single cycle programming
- MODULAR ARITHMETIC PROCESSOR
  - Fast modular multiplication and squaring using Montgomery method
  - Software Crypto Libraries in separate ROM area for efficient algorithm coding using a set of advanced functions
  - Software selectable operand length (256/512/768 bits)
- SERIAL ACCESS, ISO 7816-3 COMPATIBLE
- SINGLE 5V ±10% SUPPLY VOLTAGE
- STANDBY MODE FOR POWER SAVING
- UP TO 5 MHz INTERNAL OPERATING FREQUENCY
- VERY HIGH SECURITY FEATURES INCLUDING EEPROM FLASH ERASE
- CONTACT ASSIGNMENT COMPATIBLE ISO 7816-2
- ESD PROTECTION GREATER THAN 5000V
- 2 OPERATING CONFIGURATIONS
  - ISSUER
  - USER
- SOFTWARE SUPPORT : CRYPTOGRAPHIC LIBRARY
- FAST CRYPTOGRAPHIC FUNCTIONS PROCESSING

| | Level A ** |
|---|---|
| 512 bits signature without CRT * | 385 ms |
| 768 bits signature with CRT | 870 ms |
| 768 bits authentication (e=$10001) | 445 ms |
| 1024 bits signature with CRT | N/A |
| 1024 bits authentication (e=$10001) | N/A |

Notes * CRT: Chinese Reminder Theorem
** **Level B available soon**

**Figure 1 Pin Connection**



## INTRODUCTION

The ST16CF54, a member of the ST16XYZ family devices, is a serial access microcontroller especially designed for very large volume and cost competitive smartcards applications, where high performance Public Key Algorithms will be implemented, to cut down initialization and communication costs and to increase security.

Its internal Modular Arithmetic Processor is designed to speed up cryptographic calculations using Public Key Algorithms. It processes modular multiplication and squaring on 256/512 bit operands or a double operand of 768 bits using software. The ST16CF54 is based on an SGS-THOMSON 8 bit CPU core including on-chip memories: 480 bytes of RAM, 16 Kbytes of USER ROM and 4 Kbytes of EEPROM.

Both ROM and EEPROM memories can be configured into two sectors. Access rules from any memory section (sector) to any other are setup by the User defined Memory Access Control Matrix.

It is manufactured using the high reliable SGS-THOMSON CMOS EEPROM technology.

Reliability data related to the ST16CF54 product manufactured using SGS-THOMSON 1µ CMOS EEPROM technology confirm data retention up to 10 years and endurance up to 100,000 Erase/Write cycles.

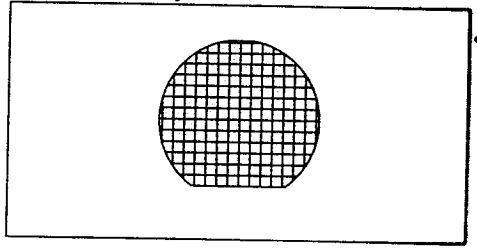
As all the other ST16XYZ family members, it is fully compatible with the ISO standards for smartcards applications.

Software development and firmware (ROM code/options) generation are done with the ST16S-EMU + ST16S-CEXT development system.

**Table 1 Contact name**

| | |
|---|---|
| CLK | Clock |
| RST | Reset |
| I/O1 | Data Input/Output |
| I/O2 | Data Input / Output (option) |
| Vcc | Supply Voltage |
| GND | Ground |

**Figure 2 Delivery form**



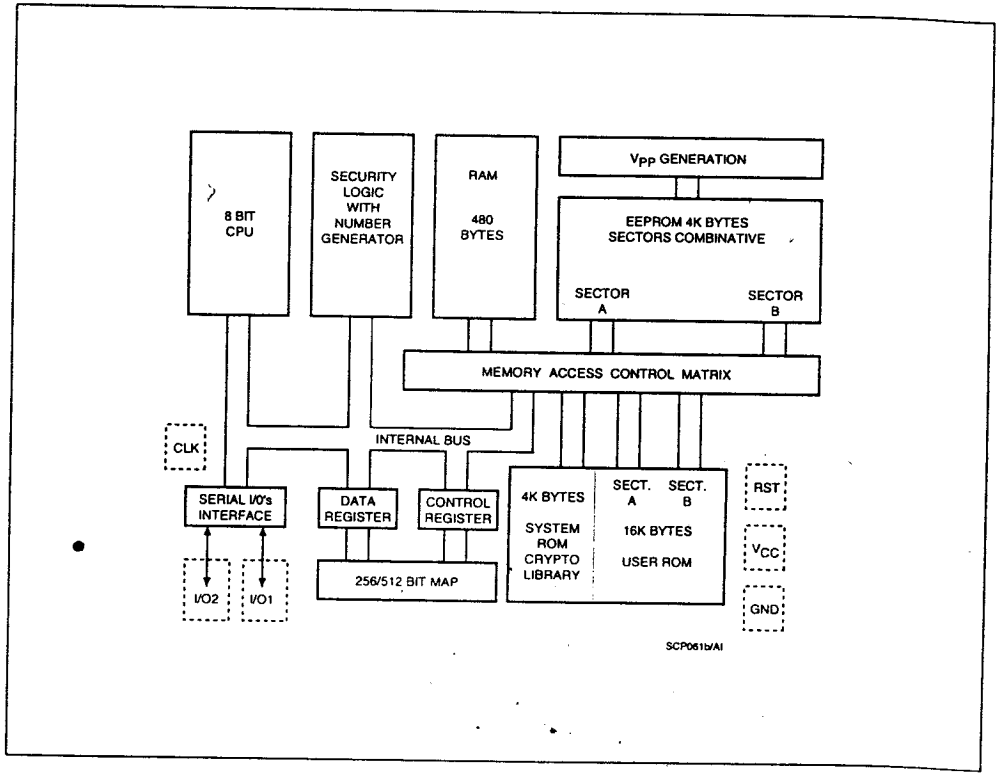
The ST16CF54 can be delivered either in unsawn or sawn wafers, 180 or 275 micron thickness.







**Figure 3 ST16CF54 Block Diagram**



# 1 FUNCTIONAL DESCRIPTION

The ST16CF54 is a serial access circuit based on a 8 bit CPU core. Operation is synchronized with an external clock that will be internally raised for driving the Modular Arithmetic Processor. See Figure 3.

The 8 bit CPU includes the ALU, the control logic, and 5 registers available to the programmer. The CPU interfaces with the on chip memories, RAM, ROM and EEPROM via the internal bus (8 data bits and 16 address bits) and through the User defined Memory Access Control Matrix.(See Chapter 7, SECURITY).

The interface between the User's Rom code and the cryptographic library is done through two full length 512 bits registers and one 32 bits register. Three types of operations: calculation of Montgomery constants, Pfield modular multiplication and Pfield modular squaring are performed by the Modular Arithmetic Processor.

From these basic calculations, modular multiplication and squaring, multiplication and squaring in normal field of numbers and modular exponentiation can be performed.

The memory mapping of the various types of memories is shown in Figure 4. RAM, ROM and EEPROM memories are directly addressable by the 16 bit address bus.

A specific logic block, named "SECURITY LOGIC" is added to this microcontroller in order to achieve an extremely high level of security against software and hardware attacks.(See Chapter 7, SECURITY).

The communication of the ST16CF54 with the interface device is made through 5 or 6 contacts:

- Vcc and GND contacts are used to power the ST16CF54
- a clock input to provide the device with an external synchronization signal (CLK)
- a reset input (RST) used to reset the internal state of the device
- a serial Input/Output contact (I/O1) which is software driven and hardware configured by User's option
- an optional secondary serial Input/Output contact (I/O2) configurable as described for I/O1.

All major functions of the ST16CF54 are driven through 8 bit control registers:

- I/O control register (P0)
- Security register (P1)
- EEPROM control register (P3)
- Configuration register (P4)
- Number Generator A (P6)
- Number Generator B (P7)

These registers are directly addressable by the CPU. See Table 2, Register description, on page 5 for the addresses of the registers.

Other registers allow the CPU to transmit commands and data to or from the MAP.






**Table 2 Register description**

| Address | Mnemonic | Name | Status after reset MSB...LSB | Status after Power on reset MSB...LSB | Bit function |
|---|---|---|---|---|---|
| 0000h | P0 | I/O Control register | xxxx xx11b | xxxx xx11b | P00 = I/O1 control<br>P01 = I/O2 control<br>P02 = unused<br>P03 = unused<br>P04 = unused<br>P05 = unused<br>P06 = unused<br>P07 = unused |
| 0001h | P1 | Security register | 0xxx 1xxxb (User config.)<br>0xxx 0xxxb (Issuer config.) | 0xxx 1xxxb (User config.)<br>0xxx 0xxxb (Issuer config.) | P10 = Vcc high detector<br>P11 = Vcc high or low detector<br>P12 = Clock detector<br>P13 = Issuer fuse status<br>P14 = Passivation or metal shield detector<br>P15 = Unused<br>P16 = Passivation or metal shield detector<br>P17 = standby mode |
| 0002h | P2 | RFU | xxxx xxxxb | xxxx xxxxb | P20-P27 = SGS-THOMSON reserved |
| 0003h | P3 | EEPROM control register | x0x0 0000b | x0x0 0000b | P30 = Programming start<br>P31 = Reset data latches<br>P32 = Erase start<br>P33 = Verify mode<br>P34 = Vpp enable<br>P35 = SGS THOMSON reserved<br>P36 = Flash Erase<br>P37 = Unused |
| 0004h | P4 | Configuration register | --xx x0xxb | 00xx x0xxb | P40 = SGS THOMSON reserved<br>P41 = SGS THOMSON reserved<br>P42 = Stop number generator<br>P43 = SGS THOMSON reserved<br>P44 = SGS THOMSON reserved<br>P45 = SGS THOMSON reserved<br>P46 = Software fuse<br>P47 = Software fuse |
| 0005h | P5 | | xxxx xxxxb | xxxx xxxxb | P50-P57 = SGS-THOMSON reserved |
| 0006h | P6 | Number Generator A | xxxx xxxxb | xxxx xxxxb | |
| 0007h | P7 | Number Generator B | xxxx xxxxb | xxxx xxxxb | |

| Address | Mnemonic | Name | Status after reset MSB...LSB | Status after Power on reset MSB...LSB | Bit function |
|---|---|---|---|---|---|
| 0008h | P8 | RFU | xxxx xxxxb | xxxx xxxxb | P80-P87 = SGS-THOMSON reserved |
| 0009h to 001Fh | | | xxxx xxxxb | xxxx xxxxb | SGS-THOMSON reserved |
| 0020h to 01FFh | RAM | RAM | Not modified | xxxx xxxxb | RAM |

**Notes:**

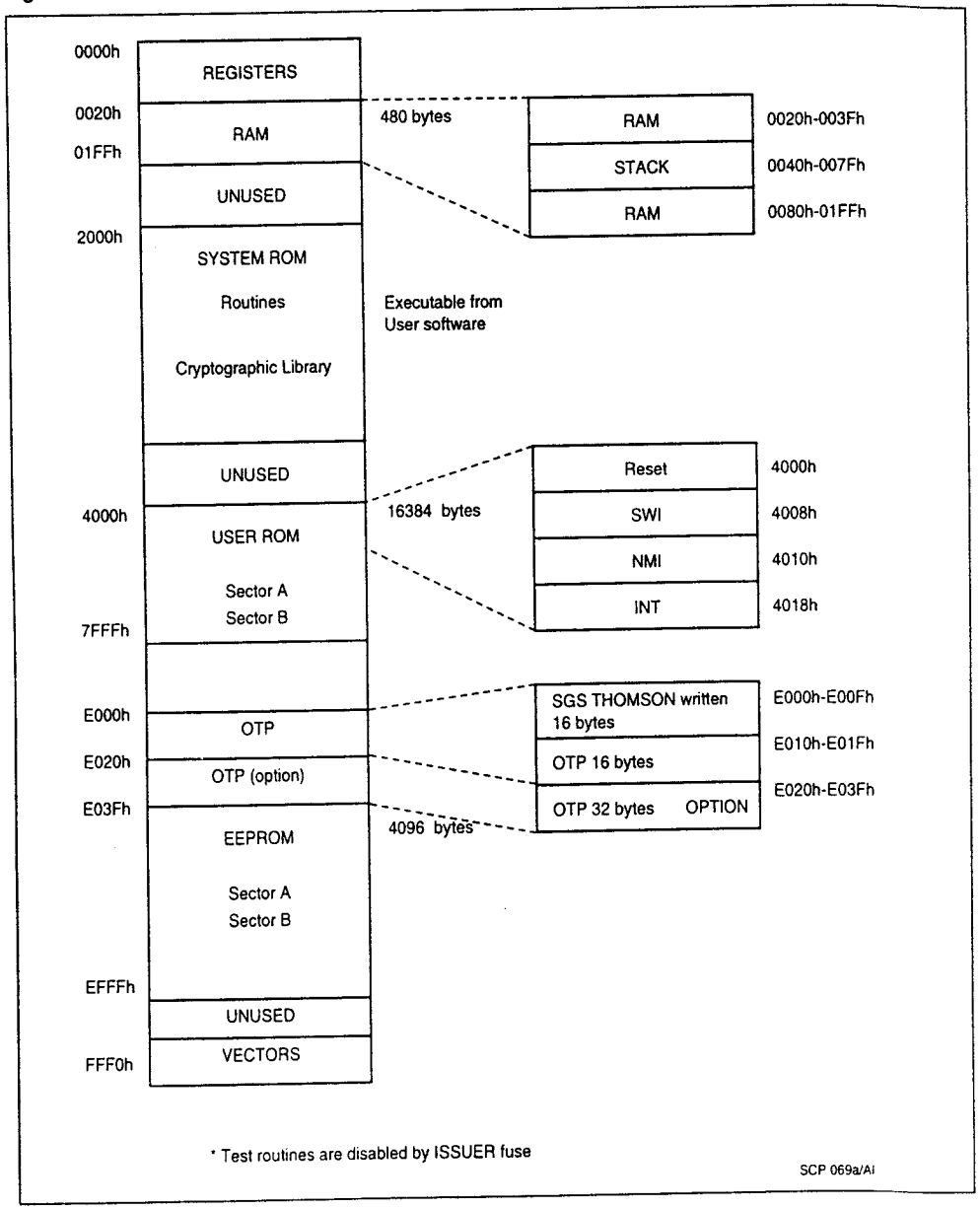
- Register bits are noted PXY: X= last digit of the address; Y= bit number; e.g. bit 3 of the security register at address 0001h is noted P13
- xxxx = undefined state
- ----- = unchanged state
- Reading unused or SGS-THOMSON reserved bits will provide undefined values. Particular attention must be paid when performing instructions such as Shift and Rotate on bytes containing one or more unused or reserved bit. Writing to these bits is forbidden.







**Figure 4 ST16CF54 Memory mapping**



## 2 SIGNAL DESCRIPTION

### CLK and RST

Refer to Figure 10 and Figure 11 for waveform and timing.

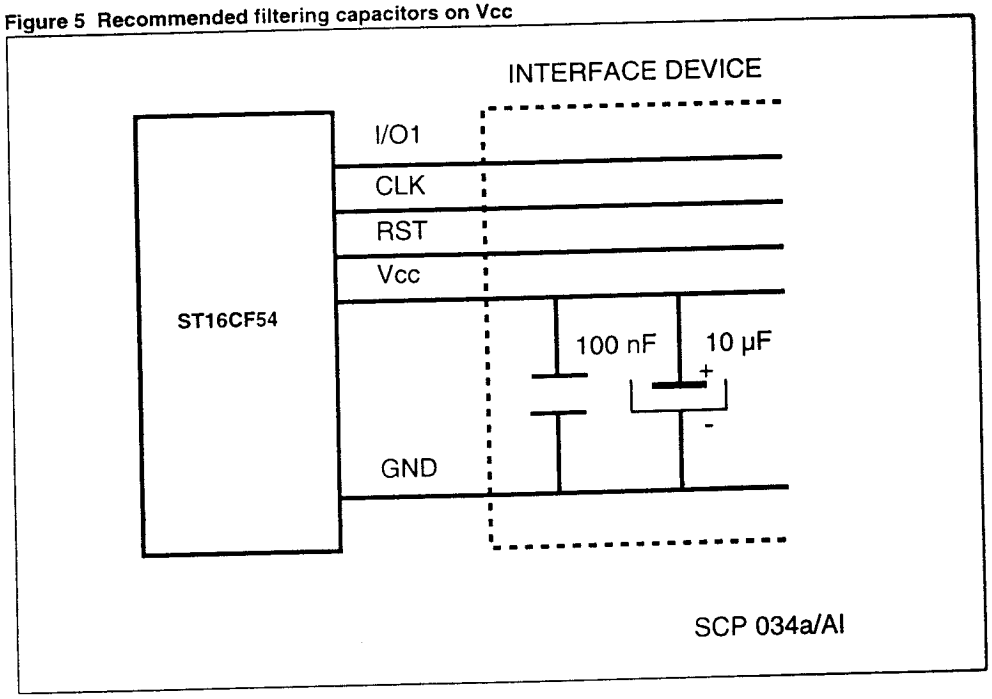
### Serial I/O

The serial I/O pins are quasi bi-directional with optional configuration on Output (OPEN DRAIN or PUSH PULL or WEAK PULL-UP). The waveform and timing are indicated in Figure 6 and in the AC Characteristics (Table 4). I/O1 is controlled through P00 (bit 0 of register P0) and I/O2 through P01 (bit 1 of register P0). I/O1 has been designed to be fully compatible with the ISO 7816-3 standard. Both I/O1 and I/O2 may be used for other asynchronous protocols.

### Vcc : Supply voltage

In order to filter spurious spikes on supply voltage pin $V_{CC}$, it is highly recommended to add decoupling capacitors on the interface device. These capacitors must be wired between GND and $V_{CC}$ as close as possible to the $V_{CC}$ pin. Recommended values for capacitors are given in Figure 5.

**Figure 5 Recommended filtering capacitors on Vcc**









## 3 OPERATING DESCRIPTION

### 3.1 EXTERNAL RESET (active LOW)

Assuming that Vcc is active and stabilized and CLK is active, when a low level is applied to the RST contact:

- the internal bus of the ST16CF54 is locked
- the CPU and MAP do not operate
- the I/O lines are set in the reception mode (bits P00 and P01 of register P0 at logical "1").

Thus the device is in low consumption mode Icc2 (See Chapter 6, LOW POWER MODES).

Then a rising edge on the RST contact resets the device and has the following actions:

- Reset bit P17 of security register P1 - standby mode disabled
- Force P13 to "1" if the ISSUER FUSE is blown
- Reset all bits of EEPROM control register P3 (See Paragraph 9.3, EEPROM, on page 31)
- Set the Interrupt mask bit (I) of Condition Code Register to "1"
- Starts the CPU at address 4000h
- Forces stack pointer at 007Fh
- Initialises the MAP for a new calculation
- Stops the MAP clock

RAM content is not affected by the external reset. (See Table 2, Register description, on page 5)

### 3.2 POWER-UP, POWER-DOWN RESET

For security purposes the ST16CF54 is reset upon a power-up and locked upon a power-down sequence. The power-up reset has the same actions as the external reset described above, leaves the RAM in an undefined state, initialises the MAP for a new calculation and resets all used bits of Configuration register P4. (See Table 2, Register description, on page 5).

In normal operations the circuit must be started using the external reset.

### 3.3 Input / Output (I/O's)

USER ROM code may use one or both of the two I/O's of the ST16CF54. The output stage circuit of the ST16CF54 can be selected by mask option (See Figure 6, I/O Contact and related circuitry, on page 10).

Three transistors T1, T2 and T3 allow the User choice of one of the following output circuits:

- T1 can be optionally used as a WEAK PULL UP (Pulling up to Vcc) or turned permanently OFF.
- T3 pulls down the I/O line as long as a logical "0" is written in P00 for I/O1 or P01 for I/O2.
- T2 can be optionally used as an active pull up for PUSH-PULL or used only to BOOST the I/O lines to "1" during 1 internal clock cycle each time a "1" is written into P0y. Boosting pulse option is used to improve the rising edge of I/O line when switching from "0" to "1". T2 can be permanently turned off to provide an OPEN DRAIN output configuration.

**Output:** Output of data is simply done by loading the data onto the corresponding bit of the I/O's control register P0. (P00 bit 0 of P0 for I/O1, and P01 bit 1 of P0 for I/O2)

**Input:** Input of data is simply done by reading the corresponding bits P00 and P01 with the prerequisite that the last output on the I/O line was a "1".

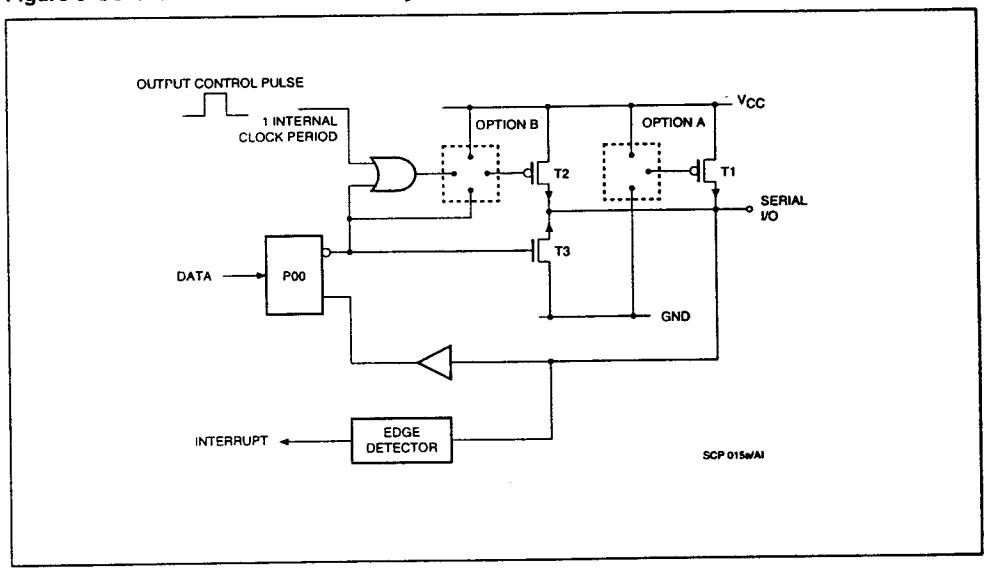
The instantaneous value of I/O line is transferred to the data bus. After a power-up sequence or a reset, the I/O control bits P00 and P01 are set to "1".

As shown in Figure 6, an edge detector connected on the Input line detects a high to low transition of the incoming data and thus can generate an interrupt upon User option.

According to the selected mask option, this start bit detection can:

- have no effect
- generate an interrupt every time a high to low transition is detected
- generate an interrupt when the circuit is in standby mode and a high to low transition is detected (see Chapter 10, OPTIONS LIST).

**Figure 6 I/O Contact and related circuitry**












# 4 ELECTRICAL CHARACTERISTICS

**Table 3 DC Characteristics 5V**

($T_A$=-25°c to 70°c; $V_{CC}$ = 5v ± 10% unless otherwise specified)

| Symbol | Parameter | Condition | Min | Typ | Max | Unit |
|---|---|---|---|---|---|---|
| $I_{cc1}$ | Supply Current | Internal Clock = 5 MHz | | 22 | 35 | mA |
| | | Internal Clock = 1 MHz | | 8 | 15 | mA |
| $I_{cc5}$ | Reduced Supply Current | Coprocessor clock stopped, PARK bit set, Internal Clock = 5 MHz | | 8 | 15 | mA |
| | | Coprocessor clock stopped, PARK bit set, Internal Clock = 1MHz | | 6 | 9 | mA |
| $I_{cc2}$ (1) | Reduced Supply Current Reset active | Internal Clock = 5 MHz | | 1 | 2 | mA |
| | | Internal Clock = 1 MHz | | 0.5 | 1 | mA |
| $I_{cc3}$ (1) | Stand-by | P17=1; STOP; External clock stopped; CLK signal low. | | 25 | 100 | µA |
| $I_{cc4}$ (1) | Reduced supply current | Number Generator stopped: P42=1, MAP parked, Internal clock running 5MHz | | 7 | 13 | mA |
| | | Number Generator stopped: P42=1, MAP parked, Internal clock running 1MHz | | 4 | 7 | mA |
| $V_{IL}$ | Input Low Voltage (CLK, RST,I/O) | | 0 | | 0.2 x $V_{cc}$ | V |
| $V_{IH}$ | Input High Voltage (CLK, RST, I/O) | | 0.7 x $V_{cc}$ | | $V_{cc}$ | V |
| $I_{IL}$ | Input Low Current (I/O) | 0v < $V_{IL}$ < 0.2 x $V_{CC}$ Open drain / No weak pull up | -20 | | 20 | µA |
| | | 0v < $V_{IL}$ < 0.2 x $V_{CC}$ Open drain / Weak pull up | | | 1 | mA |
| $I_{IH}$ | Input High Current (I/O) | 0.7 x $V_{CC}$ < $V_{IH}$ < $V_{CC}$ Open drain / No weak pull up | -20 | | 20 | µA |
| | | 0.7 x $V_{CC}$ < $V_{IH}$ < $V_{CC}$ Open drain / Weak pull up | | | 500 | µA |
| $I_{IL}$ | Input Low Current (CLK,RST) | 0v < $V_{IL}$ < 0.2 x $V_{CC}$ | -20 | | 20 | µA |
| $I_{IH}$ | Input High Current (CLK,RST) | 0.7 x $V_{CC}$ < $V_{IH}$ < $V_{CC}$ | -20 | | 20 | µA |
| $V_{OH}$ (2) | Output High Voltage (I/O) | $I_{OH}$ = -100 µA | 2.4 | | $V_{cc}$ | V |
| | | $I_{OH}$ = - 20 µA | 3.8 | | $V_{cc}$ | V |
| $V_{OL}$ | Output Low Voltage (I/O) | $I_{OL}$ = 1.6 mA | 0 | | 0.4 | V |

The voltage on all inputs or outputs shall not exceed $V_{CC}$ +0.3v or be less than -0.3v
**Note 1:** See Chapter 6, LOW POWER MODES
**Note 2:** WEAK PULL-UP or PUSH PULL options selected

### Table 4 AC Characteristics 5V

($T_A$=-25°c to 70°c; $V_{CC}$ = 5V ± 10% unless otherwise specified)

| Symbol | Parameter | Condition | Min | Typ | Max | Unit |
|---|---|---|---|---|---|---|
| $F_{CLOCK}$ | External Clock Frequency | Internal clock = External clock | 1 | | 5 | MHz |
| | | Internal clock = 1/2 external clock | 1 | | 10 | MHz |
| $t_C$ | Clock Period ($t_C = 1/F_{CLOCK}$) | Internal clock = External clock | 200 | | 1000 | ns |
| | | Internal clock = 1/2 external clock | 100 | | 1000 | ns |
| $t_{WH}$ Clock | Clock Period High | | 0.4 x $t_C$ | | 0.6 x $t_C$ | |
| $t_{WL}$ Clock | Clock Period Low | | 0.4 x $t_C$ | | 0.6 x $t_C$ | |
| $t_R$, $t_F$ Clock | Clock Rise and Fall time | | | | 0.10 x $t_C$ | |
| $t_{WL}$ Reset (1) | Pulse width for Reset | | 1 | | | µs |
| $t_{HL}$ Reset | Minimum time for Reset active after Power up | | 10 | | | µs |
| $t_{RA}$ Reset | Time from Reset high to first instruction execution | | 11 x $t_C$ | | 11 x $t_C$ | |
| $t_R$, $t_F$ Reset | Reset Rise and Fall time | | | | 500 | ns |
| $t_{SBL}$ I/O | Minimum pulse width for Start bit | | 30 | | | ns |
| $t_R$, $t_F$ I/O | I/O Rise and Fall time | Load capacitance = 50 pF (2) | | | 500 | ns |
| $t_{PROG}$ | EEPROM programming time (Erase or Program) | 1 to 32 bytes | 2.5 | | 25 | ms |
| $t_{EEW}$ | Minimum time before addressing EEPROM | | 8 | | | µs |

**Note 1**: Any pulse shorter than 100ns will be ignored
**Note 2**: PUSH PULL or BOOSTING PULSE option selected






### Table 5 Absolute Maximum Ratings

| Symbol | Parameter | Value | Unit |
|---|---|---|---|
| $V_{CC}$ | Supply voltage | -0.3 to 7.0 | V |
| $V_{IO}$ | Input or output voltages relative to ground | -0.3 to 7.0 | V |
| $T_A$ | Ambient operating temperature | -25 to +70 | °C |
| $T_{STG}$ | Storage temperature (See **Caution** page 38) | -65 to +150 | °C |
| $V_{ESD}$ | Electrostatic discharge voltage according to MIL STD 883C Method 3015, Human Body Model | 5000 | V |

**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 the specification is not implied.
Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

### Figure 7 Serial I/O Pin Signal Waveform

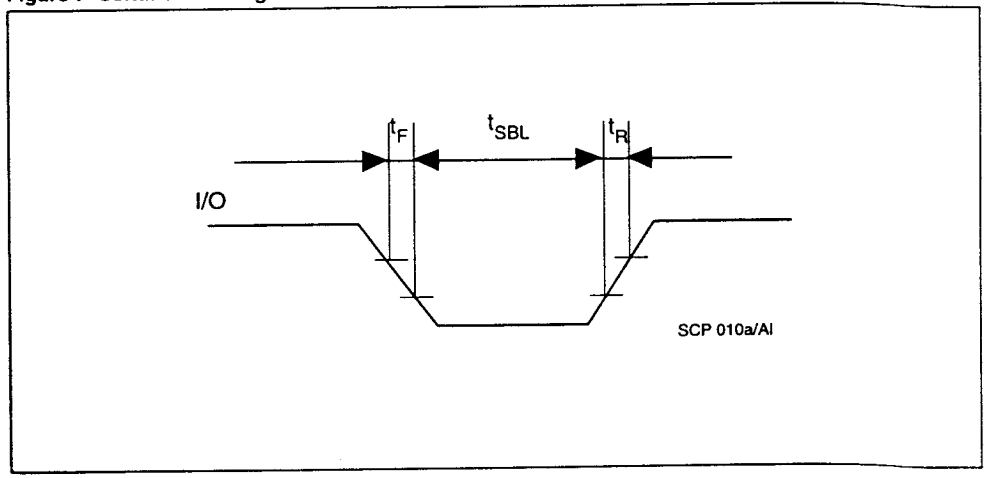


**Figure 8 INT Interrupt Timing Waveforms**

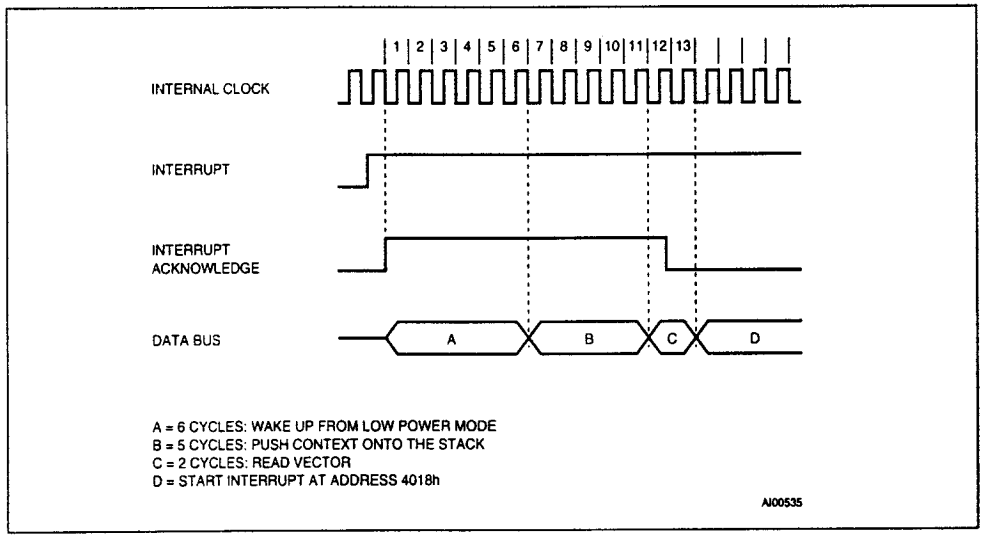



**Figure 9 NMI Interrupt Timing Waveforms**

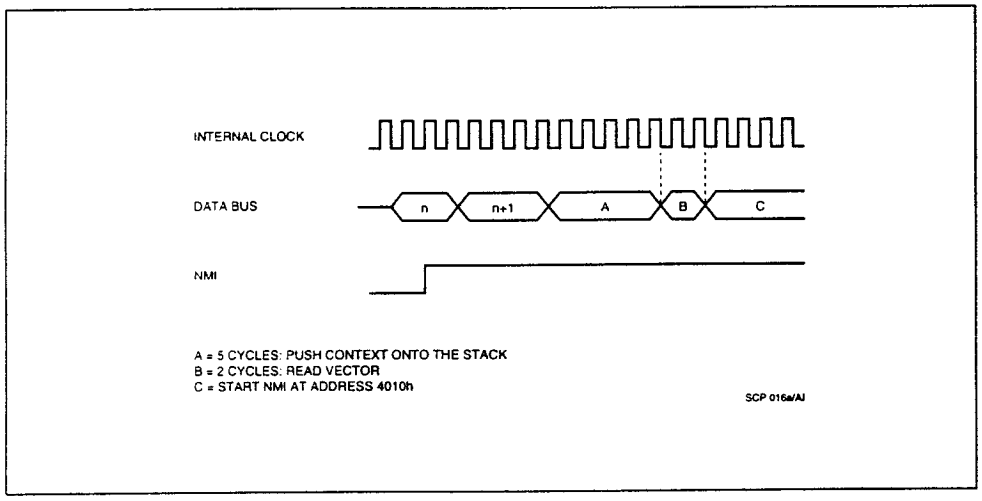









**Figure 10 Clock Pin Signal Waveform**

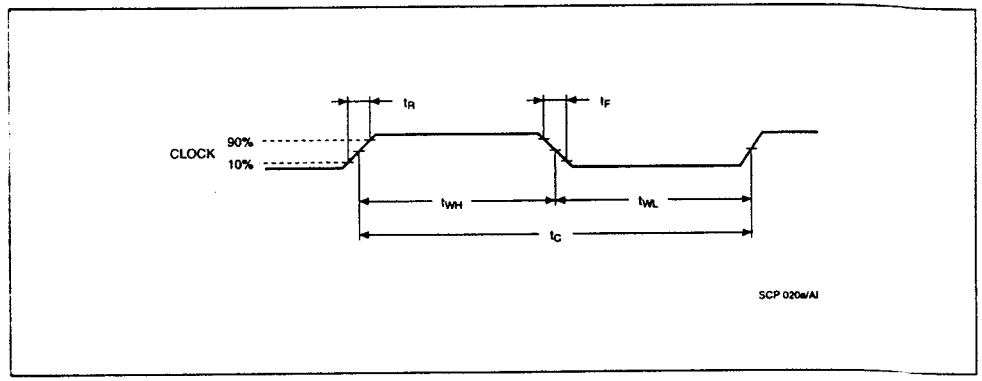
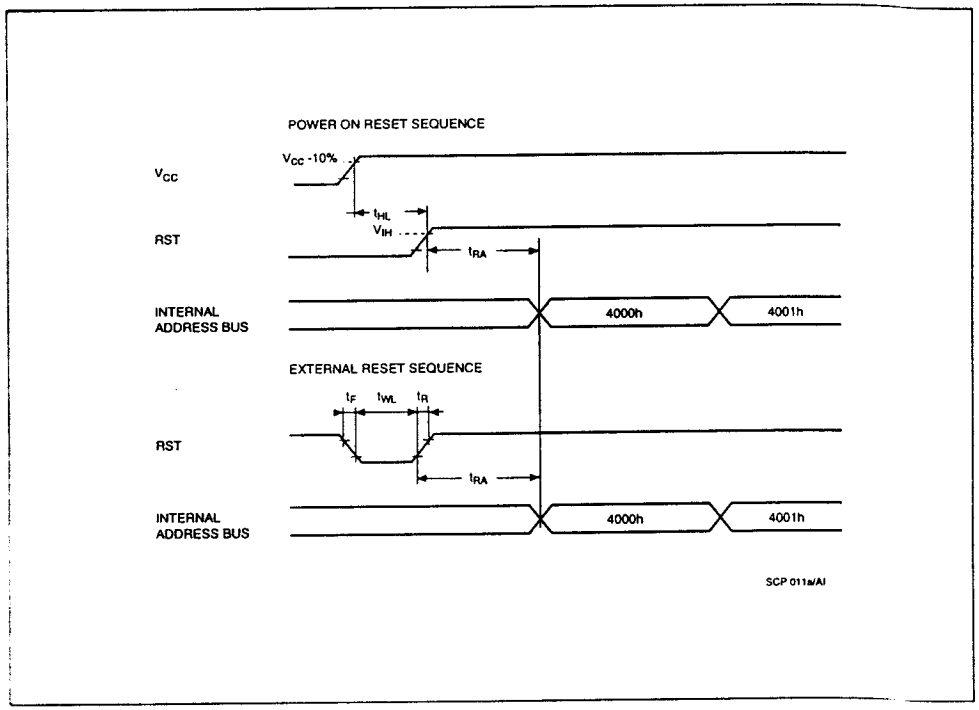



**Figure 11 Reset Pin Signal Waveform**



**AC MEASUREMENT CONDITIONS**

| | |
|---|---|
| Input Rise and Fall Times | 10 ns max |
| Input Pulse Voltages | $V_{il}$ to $V_{ih}$ |
| Input Timing Reference Voltages | 0.5 $V_{cc}$ |
| Output Timing Reference Voltages | $V_{ol}$ to $V_{oh}$ |

**Figure 12 AC Testing Input Output Waveforms**

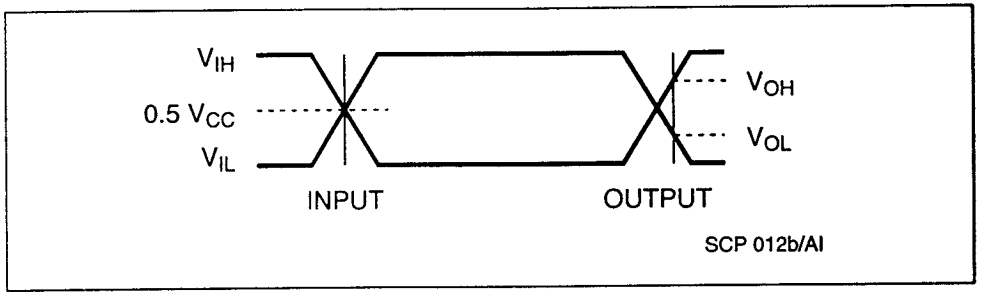



**Figure 13 AC Testing Load Circuit**

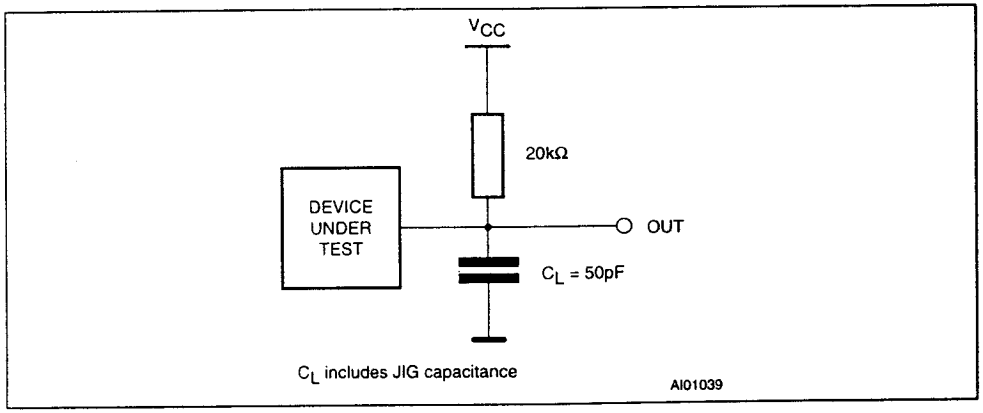



**Table 6 Capacitance**

(Ta = 25°C, f=1MHz)

| Symbol | Parameter | Test Condition | Min | Max | Unit |
|---|---|---|---|---|---|
| $C_{IN}$ | Input Capacitance | $V_{IN} = 0_V$ | | 10 | pF |
| $C_{OUT}$ | Output Capacitance | $V_{OUT} = 0_V$ | | 10 | pF |

Note: Sampled only, not 100% tested







## 5 MODULAR ARITHMETIC PROCESSOR (MAP)

Processing power necessary to rapidly and cost effectively compute cryptographic calculations using Public Key algorithms is provided by the Modular Arithmetic Processor.

The de facto standard public key algorithm is RSA, which can both decrypt and encrypt, sign and authenticate. To implement a key pair generation, one could:

- first find p and q two large prime numbers such as n=p*q
  Multiplying two prime numbers is conjectured to be a one-way function. It is easy to multiply p and q to obtain n but hard (RSA security depends upon this difficulty of factoring very large numbers) to factor n and recover the two prime numbers.
- calculate Euler function φ(n)=(p-1)*(q-1)
- ascertain one key e such that gcd (e, φ (n) ) =1
- and a second d such that e*d≡1 mod φ (n)

The public (encryption) key is e and n, the secret (decryption) key is d. Since one of the pair of keys is chosen the second one is derived. Modular exponentiation sequences are necessary to calculate $C^d$ mod n and $M^e$ Mmod n, M being the plain text, C being the cyphertext.

The MAP has been optimised to perform such modular exponentiation. The modular exponentiation, as an elementary operation, cannot be performed by the MAP, but can be flexibly made by combinations of basic operations performed by the MAP, i.e.:

- modular multiplication: A* B mod n
- modular squaring: $B^2$mod n.

Classically calculating a modular multiplication A*B mod n would entail:

- multiplying A times B, which is, usually larger than n.
- then dividing the product by the modulus n, which is the remainder.

Such divisions on very large numbers might be difficult with large number crunching processors and would be impossible to integrate onto today's Smartcards. As multiplication is a deterministic process which can more easily be implemented than division, Peter Montgomery developed a method wherein divisions can be replaced by multiplications using easily precalculated constants.

The Montgomery method is therefore based on:

- Calculation of H (first Montgomery constant)
- Calculation of $J_0$ (second Montgomery constant).
- Calculation of P(A*B)n=C (interleaved Montgomery modular multiplication reduction on Pfield multiplication)
- Calculation of P(C*H)n=A*Bmod n.

**Description of the basic operations:**

- Precalculation of Montgomery constants H and $J_0$

When n (512 bits length) is given, the two Montgomery constants H and J can be precalculated:

$H=2^{512*2}$ mod n is the first Montgomery constant.

$J_0$ is the second Montgomery constant where $J_0*n_0+1 \equiv 0 \bmod 2^{32}$.

- Presentation of the function P process (The Interleaved Montgomery reduction)

Assuming a modulus of length 512 bits and a processor with a 32 bit multiplicand, the function P process is the function P / P(T)n = T*I mod n where $(2^{512})^* I \equiv 1 \bmod n$

Calculation of P (A*B)n. Let us write A= $A_{15}$.....$A_0$

S(0)=0

For i =1,2, ,16

Step 1 $X=S(i-1)+A_{i-1}*B$, where S(i-1) is an intermediate value at the i-1th iteration and where $A_{i-1}$ is the (i-1)th block of the operand A

$X_0=X \bmod 2^{32}$

Step 2 $Y_0=X_0*J_0 \bmod 2^{32}$

Step 3 $Z=X+ Y_0*n$

Step 4 $S(i)=Z/2^{32}$, if S(i)>n then S(i) = S(i) mod n

$S(16) =A*B*I \bmod n=P(A*B)n$ with $I*2^{512}\equiv 1 \bmod n$

**Note:** To perform a modular multiplication, or a square, the P process and H the first Montgomery constant are used to retrieve from the P field to the normal field of numbers:

P(S(16)*H)n = A*Bmod n.

The Modular Arithmetic Processor, for implementing the Montgomery method to rapidly calculate a modular exponentiation, has three main registers, two (256 /512 bits length) registers and one 32 bits register:

– 2 registers B, N of 256 or 512 bits length.

– 1 register J of 32 bits length.

Specific control and data registers will allow the interface between the Central Processing Unit and the Modular Arithmetic Processor.

Using the Modular Arithmetic Processor with the appropriate firmware drivers, RSA protocols (such as signature, authentication...) can be made with moduli up to 768 bits.







# 6 LOW POWER MODES

The ST16CF54 has been designed to fit applications where security is of paramount importance. This need of performance in terms of computational power is diametrically opposed to low power consumption. As the percentage of time when the Modular arithmetic Processor computes cryptographic functions is small versus the length of a working session, low power modes will significantly reduce average power consumptions.

The power consumption can be reduced both in operating mode and in standby mode.

## 6.1 Icc1 - Reduced consumption in operating conditions

The basic way to save power consumption to use the lowest clock frequency, however this is not compatible with high speed computations.

## 6.2 Icc2 - Reduced supply current

By keeping the external reset active (low), the current consumption of the ST16CF54 is reduced and CPU is not running.

## 6.3 Icc3 - Standby mode

In order to achieve the minimum current consumption a standby mode is available. The minimum current consumption is reached when the following is performed:

– Jump to the standby routine written into the RAM which executes:

- Write a "1" into standby bit P17 (bit 7 of the security register P1) in order to desactivate the security detectors, the ROM, the EEPROM and to stop the number generator internal clock. At this step the current consumption is limited but not yet minimum.
- Execute the STOP instruction. This will halt the CPU and the internal clocks, and will also set the MAP in standby mode.

Freeze the external clock in a "0" state

P17 (standby bit of register P1) controls all static consumption of the ST16CF54 CPU and memories, while the STOP instruction controls all dynamic consumption of the CPU and MAP.

**Note:** In order to use this standby mode, the RAM of ST16CF54 must be executable. This has to be properly defined in the Memory Access Control Matrix.

To restart the circuit, it is necessary to first re-activate the external clock. Then the detection of a high to low transition on one of the I/O lines will generate an interrupt (providing this option has been selected). This interrupt will clear the standby bit P17 and will restart all CPU and MAP operations by executing the interrupt routine. An external reset can also restart the circuit, but this will execute the reset routine. The security register P1 must be reset in the interrupt routine as some bits of this register will have been set during the standby mode.

## 6.4 Icc4 - Reduced supply current in operating conditions

(Number Generator stopped)

The User has the possibility during operating conditions, to reduce the power consumption (Icc4) by disabling the number generator clock generated in the circuit. This is achieved by setting bit P42 of the configuration register P4. In this case, number generator registers P6 and P7 can be read (however the result of the read will be a fixed value), but they cannot be written.

## 6.5 Icc5 - Reduced consumption in operating conditions

When the MAP is not operating, the User can reduce power consumption of the ST16CF54 by stopping the MAP clock. This is achieved by the PARK function of the MAP.

For further details see the ST16CF54 CRYPTO LIBRARY USER MANUAL.

# 7 SECURITY

The very high security level of the ST16CF54 is the result of the combination of:

Technology
Design of the chip
Firmware
Manufacturing environment
User software

At each level the concern is to achieve the maximum performance in terms of confidentiality, integrity and availability when referring to the ITSEC (Information Technology Security Evaluation Criteria)

## 7.1 Technology and security

The integrity of the data stored into the EEPROM strongly relies on the technology used to manufacture the component. The single postillion CMOS technology used for ST16CF54 production, thanks to the very simple structure of the EEPROM cell, allows 100 000 erase and write operations on every byte. This feature is very important for applications where some bytes are updated a large number of times.

The data retention of the ST16CF54, the other key characteristic of EEPROM. covers a minimum of 10 years.

This mature technology allows stable production yields and security to the User on the availability of deliveries.

## 7.2 Security implemented at design level

In order to prevent unauthorized use of the chip or fraudulent access to data, a set of hardware security mechanisms have been implemented on the ST16CF54:

- security sensors
- Memory Access Control Matrix
- power on reset
- signal filtering
- number generators
- address scrambling
- EEPROM flash erase

### 7.2.1 Security sensors

The security sensors are accessible through the security register P1

**Table 7 Security sensors**

| P17 | P16 | X | P14 | P13 | P12 | P11 | P10 |
|---|---|---|---|---|---|---|---|

P10: Vcc high detector bit
P11: Vcc high or low detector bit
P12: Clock detector bit
P13: ISSUER FUSE status.
P14: Passivation or metal shield detector bit
P15: Unused
P16: Passivation or metal shield detector bit
P17: Standby mode bit

### Vcc detectors (P10, P11)

In order to protect the ST16CF54 against any abnormal power supply operating conditions, two kinds of protections have been implemented (see Figure 14, Vcc Detector 5V, on page 21).

A first security circuit checks if Vcc is above a Vcc High detector threshold. Bit P10 is automatically set to "1" if such a condition occurs.

A second security circuit checks if Vcc is above Vcc high detection threshold or below low detection threshold. Bit P11 is automatically set to "1" if such a condition occurs.

### Clock detector (P12)

In order to avoid step by step operations, a minimum operating frequency has been defined and is controlled by detector P12 (see Figure 15, Clock Detector, on page 21).

If the clock frequency goes under the minimum specified value, the detector will set bit P12 of the security register P1 to a logical "1", giving the user the capability to take the appropriate actions.







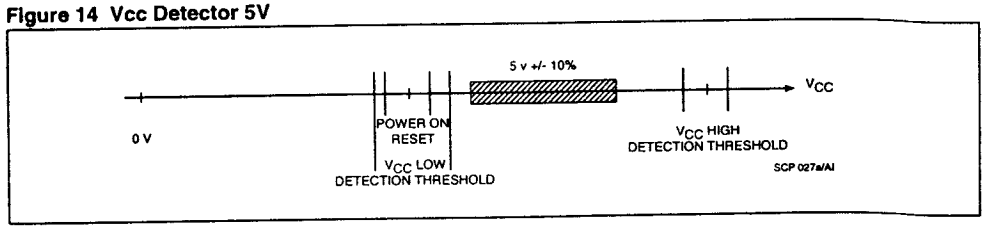

**Table 8 Vcc Detector bits**

| P10 | P11 | Detectors | Security action |
|---|---|---|---|
| 0 | 0 | No security violation detected | No action required |
| 1 | 1 | $V_{CC}$ above $V_{CC}$ high detector threshold | Action according to the security level of the application |
| 0 | 1 | $V_{CC}$ below $V_{CC}$ low detector threshold | Action according to the security level of the application |

**Table 9 Detector thresholds**

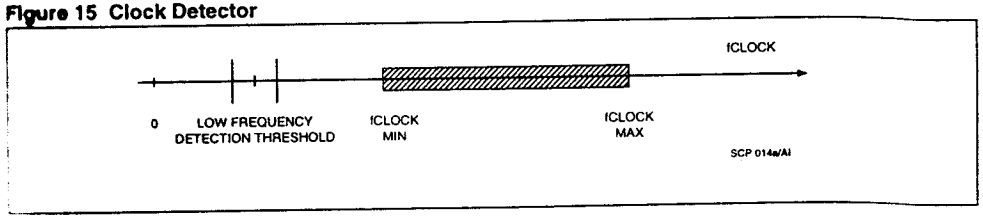
| Detector | Threshold | Conditions |
|---|---|---|
| $V_{CC}$ Low | 3.70V ± 0.75V | -25°C < $T_A$< 70°C |
| $V_{CC}$ High | 6.1V ± 0.5V | -25°C < $T_A$< 70°C |
| External clock frequency | 550 kHz ± 350 kHz | -25°C < $T_A$ < 70°C |

**Figure 14 Vcc Detector 5V**




**Note**: Products with standard voltage range option will have power-on reset detection inside the $V_{CC}$ low detection range

**Figure 15 Clock Detector**



### ISSUER fuse status (P13)

Once the ISSUER fuse has been blown the product runs in the USER configuration but can still call routines of the SYSTEM ROM. Moreover, when the ISSUER fuse is blown, the bit P13 of the security register is set to a logical "1" and will remain at "1" independant of attempt to write a "0" into P13. The goal of this bit is to indicate the state of the fuse.

### Passivation and metal shield detectors (P14, P16)

In normal operating conditions, the chip is protected by a coating and/or a package. If an attempt is made to remove the passivation layer (last level of the chip manufacturing) or the metal shield layer a specific detector will set the bits P14 and P16 of the security register to a logical level "1".

These bits P14 and P16 are provided to the User software for taking the appropriate security actions.

### Standby mode (P17)

In order to put the chip into the standby mode, the bit P17 of the security register must be set to a logical "1". When P17 is set to "1", all detectors are shut off, the on-chip ROM and EEPROM are disabled and the internal clock of the number generator is stopped (see Chapter 6, LOW POWER MODES). P17 must be set by a program running in RAM.

### P1 Register Usage

When a security sensor has triggered due to an abnormal working condition detection, a detector latch is set in order to store this event. The detector latches can be reset by software only, through the P1 security register.

The security register (P1) can be used as a read and write register. Reading the register gives directly the state of the corresponding detector latch and thus provides the programmer with "safeguarded" information.

Writing into P1 has two functions:

- Bit set:
  - * simulate the security related to a given state of a detector.
  - * put the chip in standby mode.
- Bit reset:
  If a bit of the security register P1 is at a logical "1" status due to an abnormal condition, writing to it allows this bit to be reset to a logical "0" when the abnormal condition has disappeared. Bit P13, the image of the ISSUER fuse, cannot be modified.

A chip reset leaves all the bits of the security register P1 in an undefined state except for:

- P17, standby mode, which is reset to "0".
- P13, ISSUER fuse status, which forces the state of the ISSUER Fuse into P13.

Only P17 has a hardware effect. All other detectors only warn the User Software of abnormal conditions by setting individual bits of security register P1. The User software is in charge of taking the appropriate actions.

**Caution**: For proper use and operation of the security detectors it is mandatory to follow the procedures described in the ST16xyz Application Manual available from SGS-THOMSON.







### 7.2.2 Memory Access Control Matrix

In order to protect unauthorized access to sensitive data, a Memory Access Control Matrix (MACM) has been implemented on the ST16CF54 (See Table 10). This MACM is configurable by the User during the ROM code development stage (See Chapter 10, OPTIONS LIST). Thus it is possible to prevent data stored into a memory section (SYSTEM ROM, ROM A, ROM B, EEPROM A, EEPROM B) to be dumped by a program running in another memory section.

During the fetch cycle, the address of the instruction being executed is latched. Then for all other clock cycles of the same instruction, the address bus is compared to the latched address. If the data address is not allowed from the program area through the MACM, a Non Maskable Interruption (NMI) is generated and the CPU will serve the NMI routine.

**This routine, written by SGS-THOMSON, (see Figure 17, Starter Code Sequence, on page 30) will force the CPU to execute an endless loop. Only an external reset will allow the circuit to restart.**

### 7.2.3 Power-up, power down reset

When the supply voltage applied on ST16CF54 is lower than the minimum guaranteed value, the CPU is locked. So during power-up and power-down sequences the status of the circuit is fully controlled.

The power-up reset has the same actions as the external reset described in Chapter 3, OPERATING DESCRIPTION, leaves the RAM in an undefined state and resets all bits of Configuration register P4. (See Table 2, Register description, on page 5).

In normal operations the circuit must be started using the external reset.

### 7.2.4 Signal filtering

The maximum security level of a device is guaranteed as long the behaviour of this device is controlled properly. For this reason, SGS-THOMSON has inserted a low pass filter in the RST input circuitry. Any pulse shorter than 100 ns will be ignored by the ST16CF54. The external clock signal is reshaped in order to insure that the CPU is clocked with a nominal signal.

### 7.2.5 Number generator

Random numbers are necessary for advanced authentication, signature and encryption techniques.

For this purpose a double 8 bit number generator has been included in the ST16CF54 and is accessible as a double register (P6 and P7 at address 0006h and 0007h). The values of these two 8 bits registers are independent of external signals (RST, CLK, I/O...) and give unpredictable numbers.

The operating modes are as follows:

- reading: these 2 registers P6 and P7 generate two 8 bit random numbers without correlation to each other.
- writing: Some bits of the registers P6 and P7 are set to the logical value defined by an exclusive OR between the previous logical value set in this register bit and the present data on the data bus.

**Table 10 Memory Access Control Matrix**

| PROGRAM IN | DATA IN | | | | | |
|---|---|---|---|---|---|---|
| | RAM | SYSTEM ROM | ROM A | ROM B | EEPROM A | EEPROM B |
| RAM | User | No | No | No | User | User |
| SYSTEM ROM | Yes | Yes | No | No | Yes | Yes |
| ROM A | User | No | User | User | User | User |
| ROM B | User | No | User | User | User | User |
| EEPROM A | User | No | No | No | User | User |
| EEPROM B | User | No | No | No | User | User |

It is possible to stop the internally generated clock of the number generator by setting P42 to "1" in order to save power consumption (see Chapter 6, LOW POWER MODES). In this case, number generator registers P6 and P7 can be read, the result of the read will be a fixed value, but they cannot be written. Random number generation will restart as soon as P42 is reset to logical "0".

#### 7.2.6 Address scrambling

In addition to all other security features at design level a scrambling of logical, respective to physical address of the memories has been done.

#### 7.2.7 EEPROM flash erase

In USER configuration, after a most fraudulent attempt, a specific routine is available in the SYSTEM ROM which erases all EEPROM content including OTP bytes in one erase cycle. (See Paragraph 9.2.2, SYSTEM ROM, on page 29, System ROM Library Functions). After a Flash Erase has been performed the device is logically destroyed and cannot be used any longer if User software has been written consequently. This Flash Erase security function is available if the corresponding option has been selected.

### 7.3 Security implemented by firmware

In order to allow an electrical test to be performed after embedding the ST16CF54 into packages, SGS-THOMSON has written several test routines into the SYSTEM ROM. This test operating system is active as long the ISSUER fuse is not blown and controlled by a transport key.

These routines have been written taking into account SGS-THOMSON's large experience in testing integrated circuits and are an excellent tool to ensure that the ST16CF54 has been correctly tested at the final step of assembly. This gives the guarantee that the data integrity will not be affected by an assembly defect.

SGS-THOMSON can provide the ST16CF54 with ISSUER fuse blown or not blown according to the User's request.

**The USER ROM code cannot run as long as the ISSUER fuse is not blown** (see ST16CF54 SYSTEM ROM User Manuals).

**Card manufacturers must not deliver cards without blowing the ISSUER fuse.**

### 7.4 Security at manufacturing level

A set of security procedures at every step of the manufacturing process, from application code reception to shipment, has been implemented in order to ensure the confidentiality of the application.

Only authorized people are allowed to perform sensitive operations such as electrical test, material handling from one location to another and to have access to the storage area.

Full traceability of all operations is kept for 10 years.

### 7.5 Security implemented by User's software

The security of the ST16CF54 relies on the security mechanisms implemented by hardware on the chip itself, but it is also strongly related to the User's software.

In order to optimize the User Software in terms of security, SGS-THOMSON can give some recommendations.

For proper use of the ST16CF54 security features, please refer to the ST16xyz Application Manual.







# 8 CPU

### 8.1 Introduction

The ST16CF54 CPU has a full 8 bit architecture, features a large instruction set, powerful addressing and interrupt modes, and 5 internal registers allowing efficient 8 bit data manipulation.

A list of the main features is given in Table 11, CPU Main Features, on page 26.

### 8.2 Internal Registers

The ST16CF54 CPU has five registers, as shown in Figure 16, CPU Registers, on page 26 and described hereafter:

- **Accumulator (A).** The accumulator is an 8 bit general purpose register used for arithmetic calculation and data manipulation.
- **Index Register (X).** The index register is an 8 bit register which can be used:
  - either as "second" accumulator,
  - or to create the effective address in the indexed addressing mode. This effective address is the result of the sum of the index register (X) content and an offset located within the instruction.
- **Program Counter (PC).** The program counter is a 16 bit register that contains the address of the next instruction to be executed.
- **Stack Pointer (SP).** The stack pointer is a 6 bit register that contains the address of the first free location of the stack located in the RAM. This stack is used to save the context of the CPU on subroutine calls and interrupts. After a reset, the SP is set to its upper value (007Fh) ; It is decremented after data has been pushed onto the stack and incremented after data has been popped from the stack. A subroutine return address occupies 2 locations and an interrupt saved context 5 locations.
- **Condition code register (CCR).** The condition code register is a five bit register which contains flag bits that reflect the current state of the processor, given by the results of the last executed instruction.

The condition code bits are described here below :

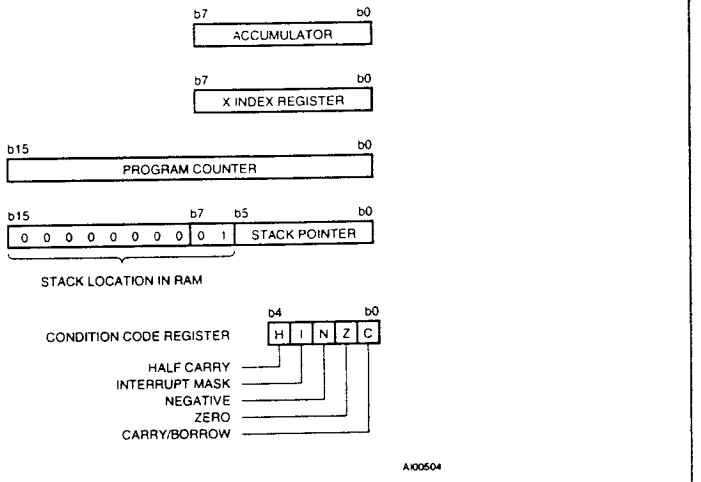
- **Half Carry (H).** The H bit is set during ADD and ADC instructions to indicate that a carry occurred between bits 3 and 4.
- **Interrupt Mask (I).** This bit is set to mask (disable) the external interrupt. If an interrupt occurs while this bit is set, the interrupt is latched and will be processed as soon as the Interrupt Mask bit (I) is cleared again.
- **Negative Bit (N).** This bit is used to indicate that the result of the last data manipulation, arithmetical or logical operation, is negative.
- **Zero Bit (Z).** This bit is used to indicate that the result of the last data manipulation, arithmetical or logical operation, is zero.
- **Carry Bit (C).** This bit is used to indicate that a carry or an overflow of the arithmetic logic unit has occurred during the last arithmetic operation. This C bit can also be set during shift, rotate and bit test instructions.

More details on the ST16xyz CPU are given in the ST16xyz Programming Manual.

**Table 11 CPU Main Features**

| SOFTWARE FEATURES | HARDWARE FEATURES |
|---|---|
| 1 to 3 bytes efficient instruction set | 8 bit architecture |
| Easy programming | 16 bit address bus |
| 10 addressing modes | Fully static operation |
| Powerful indexed addressing for tables | Low power mode |
| Full set of conditional branches | Self test mode |
| 63 basic instructions including<br>- True bit manipulation<br>- 8 x 8 unsigned multiplication<br>- TSA instruction: transfer from stack pointer into accumulator | 3 interrupt: one optional and maskable, the others non maskable<br>5 Registers:<br>- accumulator<br>- index register<br>- program counter<br>- stack pointer<br>- condition code register |

**Figure 16 CPU Registers**











## 8.3 INTERRUPTS

The ST16CF54 features both external and internal interrupts.

- The possible external interrupt is a maskable optional interrupt: INT, Detection of a start bit on the I/O
- Two internal interrupts are also available:
  - a non maskable software interrupt: SWI
  - a non-maskable interrupt: NMI, generated by the ST16CF54 Memory Access Control Matrix.

When an interrupt occurs, the registers are saved onto the stack and after the completion of the interrupt service routine, the instruction RTI (Return from Interrupt) is used in order to load the registers back from the stack (Program Counter, Index, Accumulator and Condition Code registers)

**INT**: Optional Interrupt. By mask option, the INT interrupt can be generated by the detection of a falling edge on any of the I/O lines. This interrupt is maskable, so if the interrupt is allowed (bit I of the condition code register cleared to "0"), the interrupt service routine starting at address 4018h (see Table 12) will be processed. The management of interrupt masking is performed through the instructions CLI which clears the bit I of the condition code register (interrupt enabled) and SEI which sets the bit I of the CCR (interrupt disabled). If this interrupt option is not chosen, the detection of a start bit is disabled and thus ignored by the CPU. The I bit is automatically cleared by the STOP instruction; thus enabling the interrupt on a start bit if such an option has been selected.

**NMI**: Non Maskable Interrupt. This non maskable internal interrupt (NMI) is directly driven by the MACM which controls the memory accesses (see Chapter 7, SECURITY). When this circuitry detects an unauthorized memory access, a NMI interrupt is issued and the NMI service routine starting address 4010h (See Table 12) will be processed, which will loop endlessly.

**SWI**: The Software Interrupt. SWI is an executable instruction generating a software interrupt regardless of the state of the I bit state. The interrupt service routine is located at address 4008h. (see Table 12).

The priority level of the interrupts from the highest to the lowest is:

| | |
|---|---|
| SWI | Software interrupt |
| NMI | Non maskable interrupt |
| INT | Optional interrupt |

**Table 12 Reset and Interrupt Vectors**

| Description | Vector Address |
|---|---|
| RESET | 4000 h |
| SOFTWARE NTERRUPT (SWI) | 4008 h |
| SECURITY INTERRUPT (NMI) | 4010 h |
| OPTIONAL HARDWARE INTERRUPT (INT) | 4018 h |

## 8.4 INSTRUCTION SET OVERVIEW

The ST16CF54 has an 8 bit data based instruction set that can be divided into five major groups:

- **Register/Memory and Absolute Jump group**. In this group of instructions, the operands can be the Accumulator, the Index register X or any effective memory address obtained from the different addressing modes.
  *Example*: "STA a" - means that the content of the accumulator is stored in the memory location at address "a"
- **Read/Modify group.** These instructions can read a register or a memory location, modify its content and write the new value back
  *Example*: ROR a - means that the content of the memory location a is rotated right and through the carry bit C result will be into the memory location a and the carry bit C of the condition code register.
- **Bit manipulation and Test group**. These instructions can either set, reset any bit within the first 256 memory locations, or test any bit of the first 256 memory locations and jump conditional within an 8 bit PC-relative displacement.
  *Example*: BSET b, a - sets the bit b of the memory location a.

- **PC-relative Branch group.** These instructions execute a PC-relative branch (8 bit displacement) depending on the state of some flag bits of the CCR (H, I, N, Z, C).
  *Example*: BCS ee - branch relative if carry bit C is set, displacement is ee.
- **Miscellaneous group.** These instructions are mainly control instructions on registers, stack, interrupts, subroutines and power down modes. The multiply instruction is also included in this group. This instruction performs an 8 bit by 8 bit unsigned multiplication between the index and the accumulator, the result is given in 16 bits (accumulator and index register).

The instruction set of the ST16xyz CPU is detailed in the ST16xyz Programming Manual.

### 8.5 ADDRESSING MODE OVERVIEW

The CPU uses 10 different addressing modes and thus provides the programmer with the capability of epitomizing the code in all situations.

- **Inherent**: In inherent instructions, all the information to execute the instruction is contained in the OP-code.
- **Immediate**: The operand is stored in the byte following the OP-code.
- **Direct**: The effective address of the argument is contained in a single byte following the OP-code.
- **Extended**: The effective address of the argument is contained in the two consecutive bytes following the OP-code. Instructions with extended addressing mode allow to access any location of the memory.
- **Indexed, No offset**: In this mode, the content of the index register is the effective address.
- **Indexed, 8 bit offset**: The effective address is obtained by adding the content of the second instruction byte to the appropriate index register.
- **Indexed, 16 bit offset**: The effective address is obtained by adding the 16 bits unsigned value composed by the second (MSB) and third (LSB) instruction bytes to the appropriate index register.
- **Relative**: This mode is used for branch instruction. The branch address (new value of the PC) is calculated by adding the content of the PC to the 8 bit signed value of the second byte of the instruction.
- **Bit set/clear**: This mode is used to modify a single bit of a memory location in page zero.
- **Bit Test and Branch**: This is a relative branch according to the value of a single bit of memory location in page zero. Three bytes are needed to specify this kind of instruction.

The addressing modes of the ST16xyz CPU are detailed in the ST16xyz Programming Manual.







## 9 ON CHIP MEMORIES

### 9.1 RAM

The ST16CF54 has 480 bytes of Random Access Memory (RAM) starting address 0020h. The CPU stack area is located from address 0040h to address 007Fh (64 bytes). This RAM is connected to the internal bus and is accessible to and from the CPU in an 8 bit data format. The content of the RAM is not modified after standby mode and after a reset. After a power on reset the content of the RAM is undefined.

### 9.2 ROM

The ST16CF54 has 16 Kbytes of USER ROM and 4 Kbytes of SYSTEM ROM.

#### 9.2.1 User ROM

The ROM can be split into two sectors ROM A and ROM B by option (See Chapter 10, OPTIONS LIST). The User can select one of the configurations shown in Table 13.

**Table 13 User ROM**

| ROM A | ROM B |
|---|---|
| 0 byte | 16384 bytes |
| 512 bytes | 15872 bytes |
| 1024 bytes | 15360 bytes |
| 2048 bytes | 14336 bytes |
| 4096 bytes | 12288 bytes |
| 8192 bytes | 8192 bytes |

The access rules to ROM A and ROM B sectors are defined by the Memory Access Control Matrix (See Chapter 7, SECURITY).

The USER ROM is located from address 4000h to 7FFF and must always start with the sequence reported in Figure 17, Starter Code Sequence, on page 30.

The application ROM code (file in S19 format generated by the cross assembler linker software (ST16), the OPTION LIST (see Chapter 10, OPTIONS LIST) and the personalisation must be returned to SGS-THOMSON. Immediately SGS-THOMSON will issue a ROM code verification listing, which is sent to the customer for approval. With both ROM code verification listing approval and OPTION LIST filled in, SGS-THOMSON will start realization of the prototypes (see Chapter 11, ORDERING INFORMATION.

#### 9.2.2 SYSTEM ROM

**– Test Operating System**

The SYSTEM ROM contains a test command interpreter active only when the ST16CF54 is in ISSUER configuration (ISSUER fuse not blown)

The ST16CF54 can be delivered to card manufacturers with the ISSUER fuse unblown and in this case some test modes are available to this card manufacturer. The access to this test command interpreter is restricted and subject to transport key presentation. The way to use the ISSUER test command interpreter is provided to card manufacturers on a confidential basis.

**In any case, the ST16CF54 must have ISSUER fuse blown to run USER ROM code.**

**– System ROM Library Functions**

Once the ISSUER fuse is blown, USER ROM code may call basic input/output routines, RAM test routines and the Flash Erase security function. To execute one of these functions it is only required to set some parameters in RAM (according to the desired function) and then to execute a Jump to Subroutine instruction (JSR) to the address indicated in the following table. After the execution of the function, control is returned to the User's program with some returned parameters according to the function called.

**Table 14 System ROM Library functions**

| Address | Function Name | Function |
|---|---|---|
| 23FDh | FLASH | EEPROM flash erase |
| 23FAh | RAMTST | exhaustive RAM test |
| ..... | ..... | ..... |

**NOTE:** More details on the SYSTEM ROM software and library functions are available in the ST16CF54 SYSTEM ROM User Manuals.

### 9.2.3 Cryptographic Library

This library is active when the ST16CF54 is in USER configuration. The User ROM code may call one of the cryptographic functions by setting parameters in RAM and jumping to the appropriate address in the SYSTEM ROM area. A few bytes of RAM on top of page 0 are used for managing the functions.

The input and output of parameters are given in RAM between addresses $0100 and $01FF.

See the Library User Manual for further details on parameters and operations and functions lists.

There are three main groups of functions in the library:

- Register handling: Loading and unloading functions as well as mode selection allow to initiate the MAP environment and length of operation
- Mathematical group: Basic modular or non modular operations from squaring to exponential are available for operands up to 768 bits.
- RSA related functions: Signature, authentication and key generation functions mainly are available for building cryptographic protocols.

**Figure 17 Starter Code Sequence**

The following code sequence MUST be used in order to guarantee proper product initialisation and test. It has been written for direct compatibility with the SGS-THOMSON ST16 software tools:

```
ST16                                ; external RESET starts program execution
        segment byte at 4000 ' rom' ; at ROM address 4000h.There
        BRSET P13,P1,ROMCODE        ; if fuse is blown, product is in USER mode
        JMP $2000h                  ; else, execute in ISSUER mode in $2000h
INT_SWI                             ; SWI starts at address 4008h
        segment at 4008 'rom'       ;
        BRSET P13,P1,SWINT          ; if USER mode, go to SWINT address
        JMP $2009h                  ; if ISSUER mode, go and test SWI interrupt
INT_NMI                             ; NMI starts at address 4010h
        segment at 4010 'rom'       ;
        BRSET P13,P1,NMINT          ; If USER mode, go to NMINT address
        JMP $2006h                  ; else, go and test NMI interrupt
NMINT                               ; USER mode NMI: means that
        BRA *                       ; program execution MUST STOP HERE
INT                                 ; INT starts at address 4018h
        segment at 4018 'rom'       ;
        BRSET P13,P1,INTRPT         ; if USER mode, go to INTRPT address
        JMP $200Ch                  ; else, go and test INT
ROMCODE                             ; here begins the application executable code.
        BSET P46,P4                 ; it MUST start by confirming the USER mode
CHECK_DOUBLE -RESET                 ; here can start double reset
....                                ; detection which MUST end
....                                ; by
        BSET P47,P4                 ; setting P47 before going further with security bits
                                    ; initialisation (see ST16xyz Application manual)
```









### 9.3 EEPROM

In addition to the RAM and the ROM, a non volatile memory is available in the ST16CF54. It is made up of an Electrically Erasable Programmable Read Only Memory (EEPROM) with a capacity of 4 Kbytes.

The EEPROM can be split into two sectors EEPROM A and EEPROM B by option (See Chapter 10, OPTIONS LIST). The User can select one of the configurations shown in Table 15 for the EEPROM memory.

**Table 15 EEPROM**

| EEPROM A | EEPROM B |
|---|---|
| 0 byte | 4096 bytes |
| 256 bytes | 3840 bytes |
| 512 bytes | 3584 bytes |
| 1024 bytes | 3072 bytes |
| 2048 bytes | 2048 bytes |

The access rules to EEPROM A and EEPROM B sectors are defined by the Memory Access Control Matrix (See Chapter 7, SECURITY).

The EEPROM is located from address E000h to EFFFh. A flexible and fast programming mode is provided to the User: from 1 up to 32 bytes of the same block can be programmed or erased at a time.

A block is a memory area presenting addresses with the same eleven most significant bits, that is, with the same A15-A5 address bits.

This also allows a byte per byte mode.

All the necessary programming voltage generation and control logic are included in the ST16CF54. The programming voltage generator has its own oscillator, therefore the internal programming voltage does not depend on the ST16CF54 external clock. The programming time is controlled by the software. During the programming sequence, the data and their respective addresses are temporary stored in latches.

**Any access to the EEPROM is forbidden as long as the programming sequence is not completed.**

This memory features an endurance over 100,000 erase/write cycles and data retention better than 10 years.

#### 9.3.1 EEPROM control register P3

The EEPROM programming is controlled by the 8 bit control register P3 located at the address 0003h.

**Table 16 EEPROM control register**

| X | P36 | P35 | P34 | P33 | P32 | P31 | P30 |
|---|---|---|---|---|---|---|---|

- **P30**: When set to a logical "1", P30 will start the programming session of the EEPROM if bit P34 is set to "1".
- **P31**: This bit is used to reset the EEPROM data latches: A falling edge on P31 resets the latches. One must be cautious not to bring P31 low when P30 or P32 are at "1".
- **P32**: When set to a logical "1", P32 will start the erasing session of the EEPROM if bit P34 is set to "1".
- **P33**: If set to a logical "1", will enable the "verify mode". In this mode the programmed cells are checked using the worse forced conditions to ensure correct programming.
- **P34**: Set to a logical "1", will enable the internal high voltage Vpp.
- **P35**: Reserved for SGS-THOMSON use.
- **P36**: Flash Erase. When a special sequence is followed, it is possible to erase all the EEPROM section including OTP bytes in a single operation. This allows the USER to erase all its secret information stored into the EEPROM when an abnormal condition is detected. The flash erase sequence is handled by one function of the SYSTEM ROM and bit P36 is set during this sequence. This "Flash Erase" mode may be disabled by the USER whatever the state of P36 (see Chapter 10, OPTIONS LIST).
  This mode is a security feature.

#### 9.3.2 Protected bytes (OTP bytes)

As an option, the USER can protect the first 32 or 64 bytes of the EEPROM (address E000h to E01Fh or E000h to E03Fh) against erasing (see Chapter 10, OPTIONS LIST). The first 16 bytes (from E000h to E00Fh) are programmed by SGS-THOMSON and contain traceability information.

#### 9.3.3 Erase mode

Up to 32 bytes of the same block can be erased at once (set to "0"). Erasing is performed with the following sequence:

- Check Security register P1 (see Note below)
- Set P31 (bit 1 of EEPROM control register P3) to "1" and then to "0" in order to reset the data latches.
- Write 00h at the selected address and repeat the number of times needed to erase the desired number of bytes (of the same block); up to a maximum of 32 bytes.
- Set P34 (bit 4 of EEPROM control register P3) and P32 (bit 2 of EEPROM control register P3) to logical "1" in order to enable the internal high voltage Vpp and to start the erase sequence.
- Wait for Tprog (see Table 4).
- Reset P32 and possibly P34 to "0" (if the programming voltage is no longer required).
- Wait for Teew (see Table 4) before addressing the EEPROM or its registers again.
- Check Security register P1 (see Note below) The above mentioned sequence is the only one which guarantees a proper erasure.

**Note**

For the recommended operation for highly secure application please refer to the ST16XYZ Application Manual.

#### 9.3.4 Program mode

As for the erase mode, one to 32 bytes of the same block can be programmed at once. Programming is performed with the following sequence:

- Check Security register P1 (see Note below)
- Set P31 (bit 1 of EEPROM control register P3) to "1" and then to "0" in order to reset the data latches.
- Write the required data at the selected addresses and repeat the number of times needed to program the desired number of bytes (of the same block); up to a maximum of 32 bytes.
- Set P34 (bit 4 of EEPROM control register P3) and P30 (bit 2 of EEPROM control register P3) to logical "1" in order to enable the internal high voltage Vpp and to start the programming sequence.
- Wait for Tprog (see Table 4)
- Reset P30 and possibly P34 to "0" (if the programming voltage is no longer required).
- Wait for Teew (see Table 4) before addressing the EEPROM or its registers again.
- Check Security register P1 (see Note below)

A byte must normally be erased before programming. However it is always possible to program a bit "1" over a previous "0" bit without erasing.

**Programming a "0" over a "1" is not allowed.**

The above mentioned sequence is the only one which guarantees a proper programming.

**Note**

For the recommended operation for highly secure application please refer to the ST16XYZ Application Manual.

#### 9.3.5 Verify mode

For security purposes a verify mode is proposed. The verify mode can be used to check that the programming level of data has some margin versus the normal conditions of reading.

When bit P33 of the EEPROM control register is set to "1", the verify mode is enabled. The threshold of sensing is shifted in such a way that the programmed bit at a logical "1" will be read with a more severe condition than in normal operation.

So after a programming/erasing sequence, reading data in verify mode will give the following result:

- the read data and the programmed data are the same: the writing sequence has been performed properly and the data are well programmed.
- the read data and the programmed data are different: the programming level of data is weak and the User software has to take corrective action, for example, by programming again.

The verify mode has to be used for verifying the programmed data just after a writing sequence and must be disabled (P33 ="0") in other cases for normal operation.

Verify mode shall not be used for reading erased bytes.







#### 9.3.6 Flash Erase mode

A special sequence different to the program and erase modes allows the erasure of all the EEPROM cells simultaneously, including OTP bytes (see Paragraph 9.2.2, SYSTEM ROM, on page 20).This feature can be disabled by the USER (see Chapter 10, OPTIONS LIST).

After a Flash Erase has been performed, the device is logically destroyed and cannot be used anyfurther if the User software has been written consequently.

**Indeed the User software should forbid code execution if OTP memory is erased (traceability data in the first 16 bytes, or User own data in OTP).**

## 10 OPTIONS LIST

In this product, customer options allow specific configuration to be selected. They are divided into fourteen groups (The Matrix and twelve groups numbered 1 to 12), each related to different functions. Except for the Memory Access Control Matrix definition, one and only one option may be chosen in each group.

### MATRIX CONFIGURATION

The Memory Access Control Matrix should be configured with "Y" if access is au[illegible]ed, "N" if access is denied. Each access possibility must be defined.

[redacted]

### GROUP 1 PROTECTED BYTES IN EEPROM

One of the following options has to be selected in order to protect some bytes in EEPROM (to make them behave like O.T.P.) the 16 first bytes are written by SGS THOMSON for traceability purposes.

1.1 first 32 bytes of EEPROM memory not erasable (E000h-E01Fh) ❑
1.2 first 64 bytes of EEPROM memory not erasable (E000h-E03Fh) ❑

### GROUP 2 I/O1 BUFFER CONFIGURATION

The I/O1 output buffer can have several configurations, one of which must be chosen:

2.1 I/O1 pin not used (options 2.2 and 3.1 will be assumed) ❑
2.2 I/O1 buffer has WEAK PULL UP, OPEN DRAIN output, with BOOSTING PULSE ❑
2.3 I/O1 buffer has no pull up, OPEN DRAIN output, with BOOSTING PULSE ❑
2.4 I/O1 buffer has no pull up, working always as PUSH PULL ❑
2.5 I/O1 buffer has WEAK PULL UP, OPEN DRAIN output ❑
2.6 I/O1 buffer has no pull up, OPEN DRAIN output ❑

Only options 2.2, 2.3 and 2.4 can guarantee a maximum 500ns rise time.
If options 2.3 or 2.6 are used, the card reader must provide an external PULL-UP of typically 20Kohm.
If option 2.4 is chosen, I/O1 will be an output only.

**Table 17 Memory Access Control Matrix**

| | DATA IN | | | | | |
|---|---|---|---|---|---|---|
| **PROGRAM IN** | RAM | SYSTEM ROM | ROM A | ROM B | EEPROM A | EEPROM B |
| RAM | | N | N | N | | |
| SYSTEM ROM | Y | Y | N | N | Y | Y |
| ROM A | | N | | | | |
| ROM B | | N | | | | |
| EEPROM A | | N | N | N | | |
| EEPROM B | | N | N | N | | |






### GROUP 3 I/O1 INTERRUPTS

On this I/O pin, an interrupt may be generated on the high to low transition of incoming signal (input data). One of the three following options must be selected:

3.1 NO INTERRUPT on I/O1 pin ❑
In this case, no interrupt can be generated.
3.2 INTERRUPT when in standby (P17=1) AND falling edge on I/O1 pin ❑
In this case, an interrupt will be generated ONLY when P17 is set to "1" (circuit in standby mode) AND when a high to low transition is detected on that input.
3.3 INTERRUPT at EACH falling edge on I/O1 pin (independant of P17) ❑
Every time a high to low transition is detected on this I/O1 input an interrupt is generated, independant of P17.

### GROUP 4 I/O2 BUFFER CONFIGURATION

The I/O2 output buffer can have several configurations, one of which must be chosen:

4.1 I/O2 pin not used (options 4-2 and 5.1 will be assumed) ❑
4.2 I/O2 buffer has WEAK PULL UP, OPEN DRAIN output, with BOOSTING PULSE ❑
4.3 I/O2 buffer has no pull up, OPEN DRAIN output, with BOOSTING PULSE ❑
4.4 I/O2 buffer has no pull up, working always as PUSH PULL ❑
4.5 I/O2 buffer has WEAK PULL UP, OPEN DRAIN output ❑
4.6 I/O2 buffer has no pull up, OPEN DRAIN output ❑

Only options 4.2, 4.3 and 4.4 can guarantee a maximum 500ns rise time.
If options 4.3 or 4.6 are used, the card reader must provide an external PULL-UP of typically 20Kohm.
If option 4.4 is chosen, I/O2 will be an output only.

### GROUP 5 I/O2 INTERRUPTS

On this I/O, an interrupt may be generated on the high to low transition of incoming signal (input data).

One of the three following options must be selected:

5.1 NO INTERRUPT on I/O2 pin. In this case, no interrupt can be generated. ❑
5.2 INTERRUPT when in standby (P17=1) AND falling edge on I/O2 pin. In this case, an interrupt will be generated ONLY when P17 is set to "1" (circuit in standby mode) AND when a high to low transition is detected on that input. ❑
5.3 INTERRUPT at EACH falling edge on I/O2 pin (independant of P17). Every time a high to low transition is detected on this I/O2 input an interrupt is generated, independant of P17. ❑

### GROUP 6 CLOCK

On this product, the internal clock for the CPU can be equal to the external frequency, or to its half. One of these two options has to be chosen:

6.1 Internal clock equal to external clock (NO divider) ❑
6.2 Internal clock is external clock DIVIDED by two ❑

### GROUP 7 EEPROM SEGMENTATION

The EEPROM area can be considered as 2 separated memories in terms of protection by the control Matrix. They may then have different access rules. One of the following segmentation combination must be chosen:

7.1 EEPROM area B is 4096 bytes long starting at address E000h ☐
7.2 EEPROM area A (E000h) is 256 bytes long, area B starts at E100h ☐
7.3 EEPROM area A (E000h) is 512 bytes long, area B starts at E200h ☐
7.4 EEPROM area A (E000h) is 1024 bytes long, area B starts at E400h ☐
7.5 EEPROM area A (E000h) is 2048 bytes long, area B starts at E800h ☐

### GROUP 8 ROM SEGMENTATION

The User ROM area can be considered as 2 separated memories in terms of protection by the control matrix. They may then have different access rules. One of the following segmentation combinations must be chosen:

8.1 ROM area B is 16384 bytes long starting at address 4000h ☐
8.2 ROM area A is 512 bytes long starting at 4000h, area B starts at 4200h ☐
8.3 ROM area A is 1 Kbyte long starting at 4000h, area B starts at 4400h ☐
8.4 ROM area A is 2 Kbyte long starting at 4000h, area B starts at 4800h ☐
8.5 ROM area A is 4 Kbyte long starting at 4000h, area B starts at 5000h ☐
8.6 ROM area A is 8Kbyte long starting at 4000h, area B starts at 6000h ☐

### GROUP 9 FLASH ERASE

The EEPROM content may be fully erased in one flash erase cycle, including the content of the OTP bytes. One of the following options must be chosen:

9.1 FLASH ERASE mode OFF.
The FLASH ERASE function will not erase full EEPROM ☐
9.2 FLASH ERASE mode ON.
The FLASH ERASE function will erase full EEPROM (including OTP) ☐

### GROUP 10 EEPROM PERSONALIZATION

The 16 first EEPROM bytes of each product will be personalized with SGS-THOMSON traceability data. Customer data may be written in addition. One option has to be chosen:

10.1 SGS-THOMSON personalization of 16 OTP bytes only ☐
10.2 Customer personalization required in addition to first 16 bytes ☐

### GROUP 11 DELIVERY CONFIGURATION

The ST16CF54 can be delivered in two different configurations, ISSUER or USER. One option has to be chosen. **ISSUER configuration is strongly recommended.**

11.1 ISSUER configuration ☐
11.2 USER configuration ☐

### GROUP 12 COPYRIGHT PRINTING

A copyright message can be printed on the silicon area, besides the ROM location. If chosen, printing will be: "© ROM XXX Company_name Year", where XXX, Company_name and Year are set according to the specific project, Customer and time. If the copyright option is not selected, "xxx" message only will be printed. One of following options must be chosen:

12.1 COPYRIGHT message OFF. No copyright message will appear on the circuit ☐
12.2 COPYRIGHT message printing ON. with code, name and date ☐

In order to improve test coverage, the Customer should give values expected for the Answer To Reset (ATR) if code is compatible with 7816-3 standard.

If another protocol is used, the specification of protocol and ATR value should be given with this Option List.






## 11 ORDERING INFORMATION

The SGS-THOMSON offer for microcontrollers for Smart Cards is of two types:

- User Masked chips

  Once the customer ROM code is made with the appropriate development system, the ROM code in S19 format, the filled in list of Options and the personalisation should be returned to SGS THOMSON. In any case, contact your local sales representative to get the Code Entry Procedure and the Request for Quotation Procedure (RFQ).

- SGS THOMSON Manager

  In order to speed up the access to the ST16CF54, SGS-THOMSON offers a "Manager".

  This solution, ROM masked by SGS-THOMSON allows a short cut to the ST16CF54.

### 11.1 Dual in Line Packages

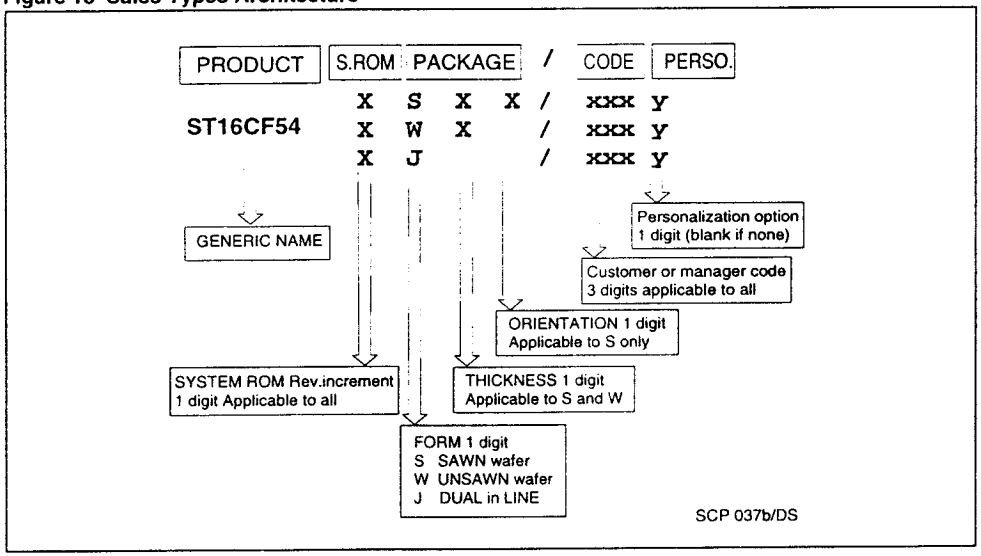
For code validation, prototypes are delivered in DUAL IN LINE package 24 pins

**Table 18 Pins references**

| PIN NUMBER | NAME |
|---|---|
| 4 | CLK |
| 5 | I/O2 (Optional) |
| 6 | RST |
| 7 | $V_{CC}$ |
| 16 | GND |
| 21 | I/O1 |

***Note***: No other pins shall be used.

**Figure 18 Sales Types Architecture**




For more details on Sales types available please contact the SGS THOMSON Sales Office nearest you.

**Table 19 Wafer Thickness**

| THICKNESS | UNSAWN | SAWN |
|---|---|---|
| 275µm ± 25µm | W2 | S2 |
| 180µm ± 15µm | W4 | S4 |

**Table 20 Sawing Orientation codes**

| ORIENTATION | CODE |
|---|---|
| GND top right | 1 |
| GND bottom right | 2 |
| GND bottom left | 3 |
| GND top left | 4 |

### 11.2 Sawing Orientation

Sawn wafers are scribed and mounted on adhesive tape into a frame. The orientation of the die with respect to the plastic frame notches has to be specified by the Customer.

The orientation is defined by the position of the GND pad of the die versus the notches of the frame, active area of product visible.

***Caution***: Wafers mounted on adhesive tape must be used within a limited period after the mounting date:

- 2 months, if wafers stored at 25°C, 55% Relative Humidity
- 6 months, if wafers stored at 4°C, 55% Relative Humidity

**Figure 19 Sawing orientation**