APPLICATION NOTE

TDA8029
Possible use of the ISO-UART internal counters

AN01010

Philips
Semiconductors

PHILIPS

Abstract

This document describes in details some of the possible uses of the internal counters of the TDA8029.

The counters are very useful to manage timing control when communicating with an asynchronous smart card either in T=0 or T=1 protocol.

The different modes of programming of these counters are explained and typical application are given for T=0 and for T=1 exchanges.

APPLICATION NOTE

TDA8029
Possible use of the ISO-UART internal counters

AN01010

Author(s):
Thierry LEJOSNE
Systems & Applications
Business Unit Identification – Business Line RIC
Caen - France

Keywords
TDA8029
Timers
Counters

Number of pages : 13

Date : 01/06/12

CONTENTS

1. INTRODUCTION

1.1 Hardware presentation

The TDA8029 single smart card reader implements a specific versatile 24 bits ETU counter for timing processing during ATR and protocol exchanges.

This counter may be used as a programmable 24 bits ETU counter (16777216 ETUs max.), or as two independent counters (one 16 bits ETU counter (65536 ETUs max.) and one 8 bits ETU counter (256 ETUs max.)).

The counters are controlled by a special register Time Out Configuration register (TOC). Different configurations may be used.

The Time Out values are loaded in the Time Out Registers (TOR1, TOR2 and TOR3), each 8 bits wide.

Once a counter is started (by an appropriate writing in the TOC register), if it is not stopped before the end of the count, it will generate an interrupt. The Uart Status Register (USR) has then to be read to know the origin of the interrupt.

Note : As the counters use an ETU timebase, it is obvious that a CLK signal is indispensable to count. Consequently, it is not possible to use the counters as long as the smart card is not powered and the card clock is running.

1.2 The different configurations

A single register, Time Out counter Configuration (TOC) is used to configure the working mode of the counter

It may be used as a single 24 bits counter or as two independents (TOR3+TOR2 as a 16 bits counter and TOR1 as a 8 bits counter)

1.2.1 Definitions

Each counter may be configured in 3 ways :

- software mode : the count starts as soon as the mode is configured in the TOC register and an interrupt is generated at the end of the count.
- start bit mode : the count starts as soon as a start bit on the I/O line has been detected (in transmission or reception mode). An interrupt is generated at the end of the count.
- autoreload mode : the count starts as soon as a start bit on the I/O line has been detected (in transmission or reception mode) and generates an interrupt at the end of the count. Then the count

starts again with the initial count value and generates an interrupt each time the count is reached till it is not stopped by writing the appropriate value in the TOC register.

Furthermore, a special mode can be used to stop all the timers after the 12th ETU following the first received start bit detected on the I/O line after this mode has been programmed by writing in the TOC register. This mode is called auto-stop in the following tables. This feature may be very useful during the ATR processing (cf. §2.1).

1.2.2 Two independent counters

Here are presented the possible TOC register values to work with two independent counters.

TOC	TOR3	TOR2	TOR1
0x00	stopped		stopped
0x05	stopped		start bit autoreload
0x61	soft		stopped
0x65	soft		start bit autoreload
0x85	stopped		start bit autoreload auto-stop
0xE5	soft auto-stop		start bit autoreload auto-stop

1.2.3 One 24-bits counter

Here are presented the possible TOC register values to work with one 24-bits counter.

TOC	TOR3	TOR2	TOR1
0x00	stopped		
0x68	soft		
0x7C	start bit		

1.2.4 Changes rules

The following rules have to be respected to assure a good operation of the counters :

- if a previous software count is not reached, one has to stop the concerned counters before restarting a software count.
- the TORs registers can be changed during a count only in case of a single 24-bits start bit counter configuration.
- It is forbidden to write a value in the TOC register when the card clock is not running.

2. EXAMPLES OF USE OF THE COUNTERS

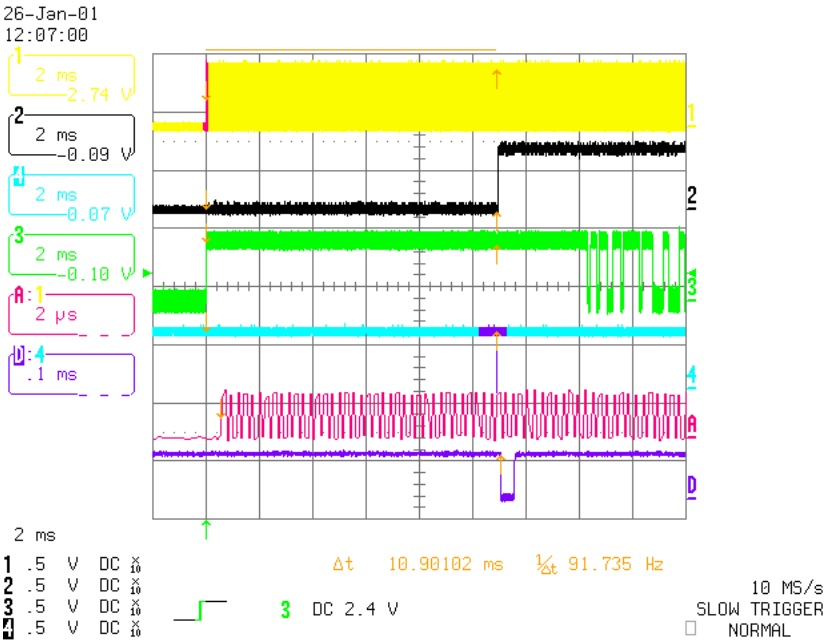
1.3 During the ATR of the card

The activation of a card is somewhat different in ISO mode or in EMV mode. In particular, the total Answer To Reset duration of the smart card should not exceed 19200 ETUs in EMV mode as it not specified in ISO mode. The two cases are detailed hereafter.

1.3.1 Activation in ISO mode

In case of a cold reset, after having applied CLK, the reader has to maintain RST in low state for a period of between 40000 and 45000 clock cycles before to set RST in high state.
This timing control can be achieved using counters 2 + 3 in software mode (it could be done also using one 24-bits counter) :

- load TOR3=0x00 and TOR2=0x6C, i.e. 108 ETUs = 40176 clock cycles ⊂ [40000 ; 45000] clock cycles
- program the Time Out Configuration register (TOC) to work in software mode (T3+T2) : **TOC = 0x61**
- set START bit in PCR to 1
- wait for a TO3 interrupt
- set RSTIN bit in PCR to 1

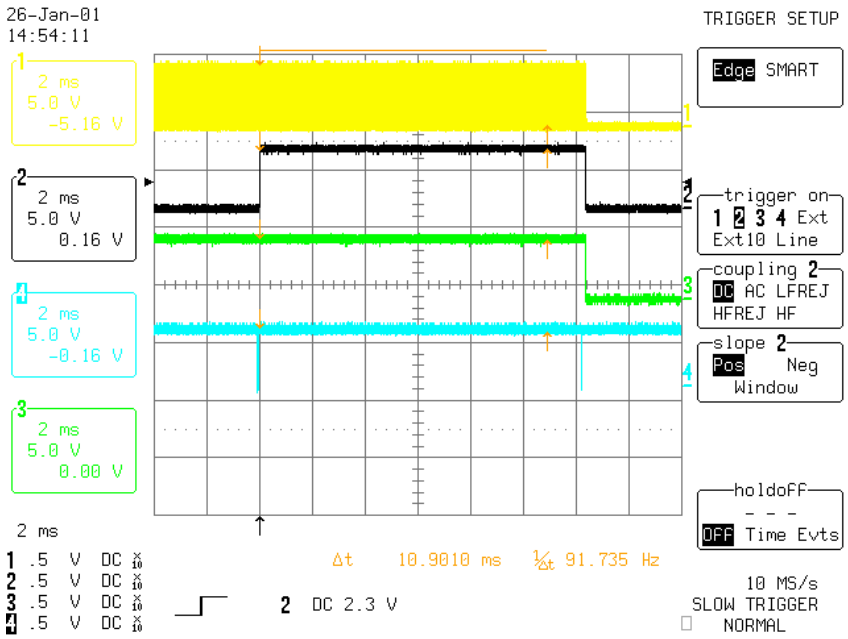


1 (A) CLK
2 RST
3 I/O
4 (D) INT0

This figure shows the TO3 interrupt corresponding to the 108 ETUs count after the first clock cycle. Then the bit RST can be set to 1.

Then, the answer to reset from the card must begin between 400 and 40000 clock cycles. Once more, timer 2 + 3 in software mode may be used to check this timing.

- load TOR3=0x00 and TOR2=0x78, i.e. 120 ETUs. These 120 ETUs include first received character, that means that the time between the TOC write operation and the leading edge of the start bit of the first received character should not exceed 108 ETUs, i.e. 40176 clock cycles. Due to the ETU resolution of the counters, that is the best approximation that can be done to check this timing.
- program the Time Out Configuration register (TOC) to work in software mode (T3 + T2) : **TOC=0x61**
- if a character reception has not been detected before the end of the count, the card can be considered as mute.



1 CLK
2 RST
3 I/O
4 INT0

This figure shows the TO3 interrupt corresponding to the 120 ETUs count after the bit RST has been set by software. In our case, the card has not given its answer to reset during that time interval ; it can be considered as mute and it is consequently deactivated.

- If a character is received before the end of the count, one have to stop the timers 2 + 3 (**TOC=0x00**), reload the TOR to check 9600 ETUs between every received character (TOR3=0x25, TOR2=0x80) and at last reload the TOC register with the same value (**TOC = 0x61**).
- Once the complete ATR has been received, all the timers have to be stopped (**TOC = 0x00**).

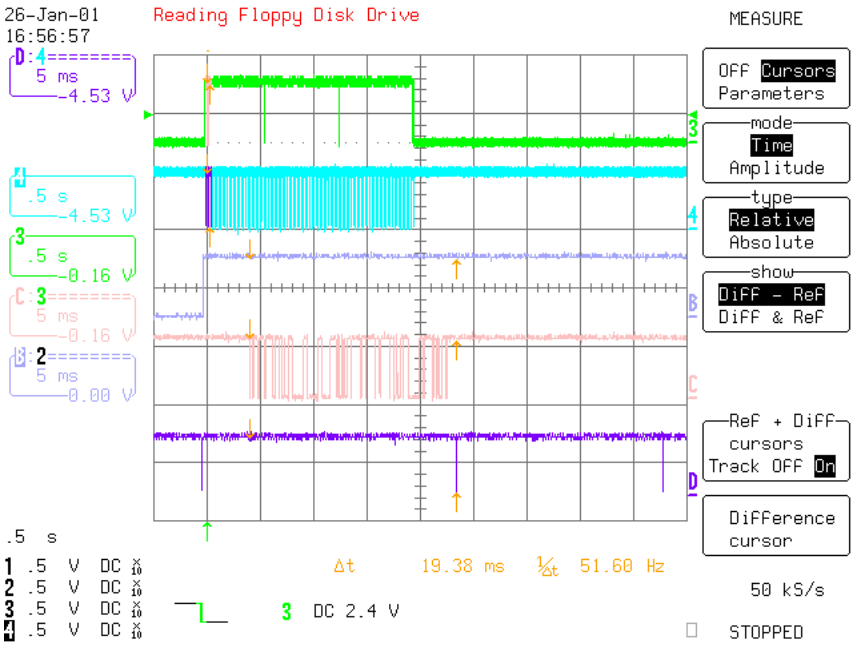
1.3.2 Activation in EMV mode

In case of EMV compliant activation, the complete time duration of the complete ATR has to be checked (no more than 19200 ETUs). In that case, the timer 1 may be programmed to give an interrupt every 192 ETUs (0xC0) and then the software has to verify than no more than 100 TO1 interrupts have occurred during the total time of ATR reception.
Before receiving the last character of the ATR, a special mode may be used which automatically stops all the timers at 12 ETUs after next the start bit detected on the I/O line. That is what we called auto-stop mode in §1.2.1.

Consequently, the sequence described above is changed as follows :

- load TOR3=0x00 and TOR2=0x6C, i.e. 108 ETUs = 40176 clock cycles ⊂ [40000 ; 45000] clock cycles
- program the Time Out Configuration register (TOC) to work in software mode (T3+T2) : **TOC = 0x61**
- set START bit in PCR to 1
- wait for a TO3 interrupt
- set RSTIN bit in PCR to 1
- check [400, 42000] clock cycles ATR beginning : TOR3=0x00, TOR2=0x78, TOR1=0xC0 and **TOC=0x65**
  Timer1 is also used to begin the 19200 ETUs count after the first received character
- after every received character except the one before the last one, reload the timers to check 9600 ETUs and 19200 ETUs :

  TOC=0x05 *Counter 1 continues to count in autoreload mode*
  TOR3=0x25, TOR2=0x80, TOR1=0xC0
  TOC=0x65 *Counters 2+3 begin a new software count*



(B) RST
3 (C) I/O
4 (D) INT0

This figure shows the TO3 interrupt (the first one on channel D) corresponding to the 108 ETUs count to set the RST line.

The following interrupts correspond to the repetitive 192 ETUs count after the first start bit detected on the I/O line. In our case, the card has not given its complete answer to reset before the 100th interrupt and it is consequently deactivated.

- before receiving the last character of the ATR, use the special End of ATR mode (auto-stop) :

TOC=0x05	*Counter 1 continues to count in autoreload mode*
TOR3=0x25, TOR2=0x80, TOR1=0xC0	
TOC=0xE5	*Counters 2+3 begin a new software count* *All the counters will be automatically stopped 12 ETUs after the next start bit detected.* *In case of an ATR which length is very close to 19200 ETUs, the time to manually stop the timers could be too long and therefore a fake alarm could be detected.*

1.4 During an exchange in T=0 protocol :

In T=0 protocol, as the extra guard time used to send characters from the interface device to the card may be automatically managed by the ISO-UART hardware by the means of the GTR register, the only timing to check is the Work Waiting Time (**WWT**).

- During a transmission phase to the card, timers may not be used. It is nevertheless advised to load the TOR with the values that will be used during the reception phase (WWT) to gain time
- Before to set the UART in reception mode, the timers have to be programmed to check the WWT. The value of the WWT (960*WI*D) is loaded in the TOR321 and the timer mode is programmed to be a single 24 bits counter, starting counting on the first start bit detected on I/O (**TOC=0x7C**)
- If a TO3 interrupt occurs during the reception, that means that a time-out error has been detected and the card has to be deactivated
- Else after having received the last character from the card, the timers have to be stopped (**TOC=0x00**).

1.5 During an exchange in T=1 protocol :

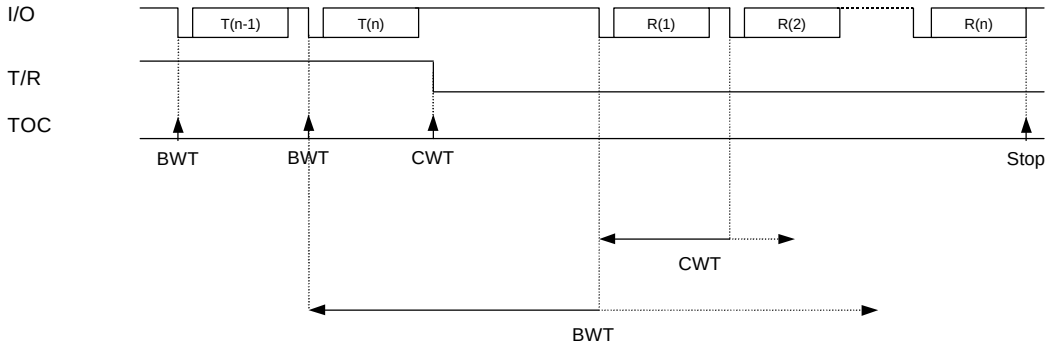
In T=1 protocol, several timings have to be checked :

- Character Waiting Time (**CWT**) defined as the maximum delay between the leading edges of two consecutive characters in the same block,
- Block Waiting Time (**BWT**) defined as the maximum delay between the leading edges of the last character sent by the TDA8029 and the first character received from the card,
- Block GuardTime (**BGT**) defined as the minimum delay between two consecutive characters in opposite directions. This timing control can be done using the BGT bit in MSR register specifically designed for that.

Anyway, the following process can be achieved to check **CWT** and **BWT** :

- Before a transmission phase to the card, timers may be programmed to check if the **BWT** will be respected by the card at the end of the transmission.
  For that, TOC must be programmed to work in a single 24 bits counter starting on start bit (**TOC=0x7C**) and TOR321 must be loaded with the current BWT value. Thus, the timers will restart to count BWT on the start bit of every character sent to the card and in particular on the start bit of the last character sent.
  If a TO3 interrupt occurs before the reception of a character, a time-out error will be generated.
  As the TDA8029 is the master of the exchange with the smart card, the CWT is not checked during transmission.
- Immediately after having sent the last character to the card, the TOR321 registers have to be reloaded with the values corresponding to the **CWT** parameter of the card. This count will effectively start when the first received byte from the card will arrive.
  In the same way, if a TO3 interrupt occurs before the reception a character, a time-out error will be generated.
- After having received the last character from the card, the timers have to be stopped (TOC=0x00)

The timers management can be illustrated as follows :



1.6 Possible other applications

Others counters applications are imaginable.
The only restriction is, as mentioned before, to keep in mind that they only can be used when the card is powered, i.e. with a running clock card.

For instance, for cards supporting clock stop, ISO 7816 specifies :

- CLK can be stopped only 1860 clock cycles after the last received character from the card,
- the first character sent by the TDA8029 after the restart of the clock should not be send before 700 clock cycles

Depending on the current ETU duration, the clock cycles counts may be approximated using counters in software mode.