The Analysis of Microprocessor Instruction Cycle

Andrzej Kwiecień, Michał Maćkowski, and Krzysztof Skoroniak

Silesian University of Technology, Institute of Computer Science,
Akademicka 16, 44-100 Gliwice, Poland
{akwiecien,michal.mackowski,krzysztof.skoroniak}@polsl.pl
http://www.polsl.pl/

Abstract. Each microcontroller realizing the code saved in a program memory emits electromagnetic disturbances, both conducted that propagate through lines connected to the processor and radiated in the form of electromagnetic field. All of these undesirable signals emitted by the processor can be measured, received and interpreted by the appropriate methods. However, this subject requires a precise measurement and understanding of processes occurring inside the microprocessor during realization of the sequential instructions. The presented results of the influence of parameters such as data bus state, instruction argument, the result of operation on the voltage waveform on the power supply lines of microprocessor, enable to understand the processes occurring during the realization of following instructions by microprocessor unit.

Keywords: reverse engineering, program code, microcontroller, conducted emission, electromagnetic disturbances, electromagnetic interference.

1 Introduction

The analysis of microprocessor programme code on the basis of measurement of power supply changes, requires an accurate measurement of voltage or current draw by the processor during execution of the instruction cycle. Temporary changes in power consumption during the execution of following instructions are mainly due to having to reload the output capacity of gates within the structure of microprocessor [1]. Total current, used by all gates in the microprocessor unit when changes of the output state occur, can take very high values, and its amplitude and the waveform may enable the analysis and reconstruction of processes occurring in the considered system. The network controller placed in the network card can be also considered as a microprocessor unit, which is responsible for data processing of transmitted frames.

The microprocessor executing a program, performs certain repetitive activities consisting in getting instruction codes from the memory and loading them into the microprocessor control system, and then executing the fetched instruction. All these operations executed by microprocessor are synchronised by a clock signal, which result in an increased activity of elements constituting the central unit

A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2011, CCIS 160, pp. 417–426, 2011.

in each machine cycle. Mainly, the activity of address and data buses, instructions decoder and arithmetic logic unit, causes the changes of outputs states of gates included in these elements, and thereby contributes to the dynamic power consumption from the power source. A precise analysis of voltage changes during the performance of particular machine cycles included in a single instruction cycle, presented in the paper, may allow to determine which instruction is currently executed [2,3,4].

2 Test Bench

The test bench presented in the Fig. 1 consists of microprocessor PIC16F84A produced by Microchip to which an 250 kHz external square waveform generator was connected. Programmer used in the research was connected to the microprocessor only while programming occurred, in order to avoid conducted disturbances. Otherwise, these disturbances can spread from the programmer on the microprocessor supply lines. During the research the test bench was placed in shielded environment – GTEM (Gigahertz Transverse ElectroMagnetic) cell, which ensured an entire isolation of measurement area from the external influences of electromagnetic fields. The microprocessor was powered with 5 V from Agilent power supply (E3649A). In previous studies a complete of batteries was used, however a long time of research resulted in discharging them, and as a consequence, caused a large error of measured voltage.

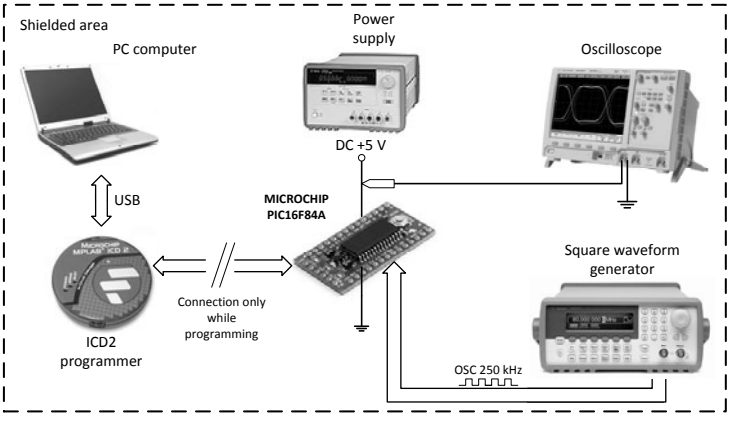

Fig. 1. The schema of research position

The analysis of microprocessor programme code based on the observation of power supply changes, requires a precise measurement of voltage or current draw by the processor. Each change of gate state determines a temporary change in power consumption by the microprocessor unit, meanwhile the total power drawing by all gates that execute a single instruction may indicate the kind of instruction, which is already executed.

Figure 2 presents three cases of the current/voltage measurements that were considered as follows:

- Measure 1 (Fig. 2a) – measured parameter is the voltage drop on the resistor placed on the processor ground circuit. Nevertheless, in this case the problem concerns an appropriate selection of resistance. Too little resistance causes that measured voltage has very little value (at the noise level),whereas too high a resistance value lowers the voltage that powers microprocessor itself, and as a result its incorrect work.
- Measure 2 (Fig. 2b) – measured parameter is the voltage drop on the secondary winding of the transformer. The primary winding is in the microprocessor ground circuit. An additional element in the form of transistor causes too much uncertainty of measurement therefore, this method was not taken into account during the research.
- Measure 3 (Fig. 2c) – an oscilloscope was connected to the supply line in order to observe the voltage drop on them. Despite of using the linear (stabilized) power supply, the voltage drops was observed in the oscilloscope, which were an accurate reflection of current flowing through power lines. The DC power supply was unable, in this case to ensure a constant level of voltage because of too low rate of output voltage stabilisation, in comparison with the transient and rapid changes in current drawn by the microprocessor, when the gate switching occurred. This method has proved to be the best, and therefore was used in the research. This approach was dictated by the difficulty in finding a proper current probe, which could measure the currents of a milli, and even microampere, with sampling frequency of 1 GHz.

3 The Research Procedure

The research procedure is as follows (Fig. 3):

1. Assignment of the value to the working register and accumulator.
2. Determination of the time flow of the microprocessor power supply voltage during the whole program.
3. Excision of part of the time flow which refers to the currently tested instruction.
4. Determination of influence of parameters such as: data bus state, instruction argument, the result of operation on the voltage flow measured on the microprocessor supply lines, when the instruction is executed.

Each program consists of 11 instructions:

- the instruction that initializes the microprocessor, realized implicitly – microprocessor initialization,
- the instructions that reset the value of accumulator and the working register (two instructions),
- the instructions that set the state of a working register and accumulator (three instructions),

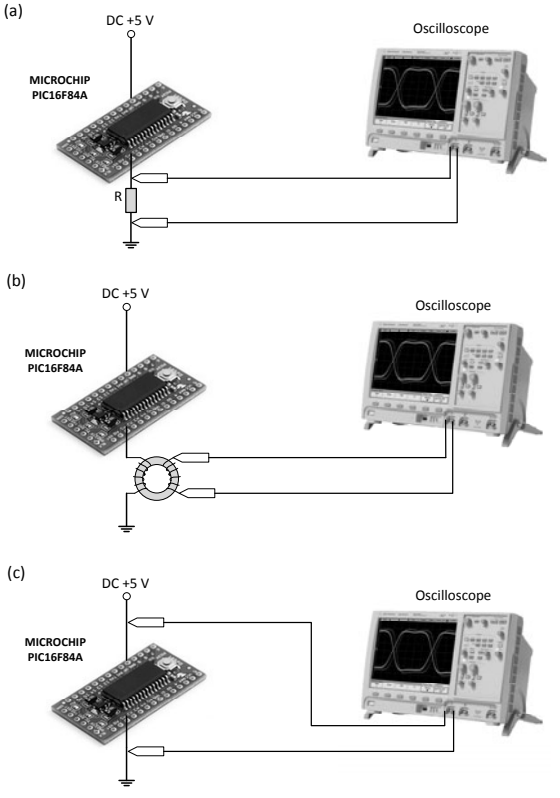

Fig. 2. The way of connecting the oscilloscope during the research

- the tested instruction,
- the instructions that set the state of a working register and accumulator (three instructions),
- the SLEEP instruction that was to switch the microprocessor into standby mode.

In order to execute the instructions that set the working register and accumulator on a certain value, it is necessary to use the data bus and arithmetic logic unit. Thus, before the tested instruction is executed, the state of the basic elements included in microprocessor results from the realization of previous instructions. There were two tests conducted during the research for six programmes (instruction arguments are presented in decimal system):

1. The influence of instruction argument and the state of data bus resulting from the previous operation on voltage waveform during the first machine cycle. This test concerns the MOVLW instruction (bold type in Table 1).

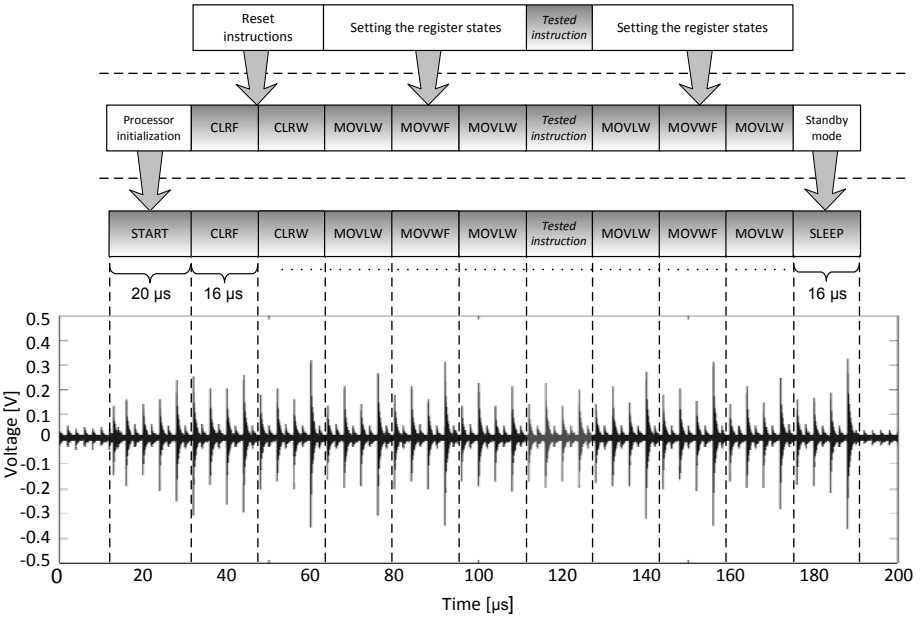

Fig. 3. The research procedure – microcontroller test program construction

2. The influence of instruction operation result and the state of data bus on voltage waveform during the third machine cycle. In this case the tested instruction is ADDLW (bold type in Table 2).

4 The Research Results

Figures 4, 5 and 6 present the voltage waveforms on the microprocessor supply lines in the middle of executing MOVLW . 0, MOVLW .12, MOVLW .15 instructions, respectively for programmes 1, 2 and 3 (Table 1). Comparing the voltage waveforms in the figures it can be seen that mainly the differences during the first machine cycle occur. The voltage shapes for 2, 3 and 4 cycle are the same for all considered instructions. In order to explain the differences observed during the first machine cycle, it is necessary to examine the state of microprocessor before and afterwards the first machine cycle execution.

Before the first machine cycle of the tested instruction is realized, a state resulting from the previous instruction is maintained on the data bus. In the following stage, an instruction is decoded, and instruction argument contained in the instruction code or retrieved from memory is set on the data bus, overwriting at the same time its previous state (Table 3).

Figures 7, 8 and 9 present the voltage waveforms on the microprocessor supply lines in the middle of executing ADDLW .63, ADDLW .12, ADDLW .85 instructions, respectively for programmes 4, 5 and 6 (Table 2). Comparing the

Table 1. Microprocessor test programmes – interaction on the first machine cycle

Program 1	Program 2	Program 3
CLRF 15	CLRF 15	CLRF 15
CLRW	CLRW	CLRW
MOVLW .0	MOVLW .0	MOVLW .0
MOVWF 15	MOVWF 15	MOVWF 15
MOVLW .0	MOVLW .3	MOVLW .240
MOVLW .0	**MOVLW .12**	**MOVLW .15**
MOVLW .0	MOVLW .0	MOVLW .0
MOVWF 15	MOVWF 15	MOVWF 15
MOVLW .0	MOVLW .0	MOVLW .0
SLEEP	SLEEP	SLEEP

Table 2. Microprocessor test programmes – interaction on the third machine cycle

Program 4	Program 5	Program 6
CLRF 15	CLRF 15	CLRF 15
CLRW	CLRW	CLRW
MOVLW .0	MOVLW .0	MOVLW .0
MOVWF 15	MOVWF 15	MOVWF 15
MOVLW .0	MOVLW .36	MOVLW .85
ADDLW .63	**ADDLW .12**	**ADDLW .85**
MOVLW .0	MOVLW .0	MOVLW .0
MOVWF 15	MOVWF 15	MOVWF 15
MOVLW .0	MOVLW .0	MOVLW .0
SLEEP	SLEEP	SLEEP

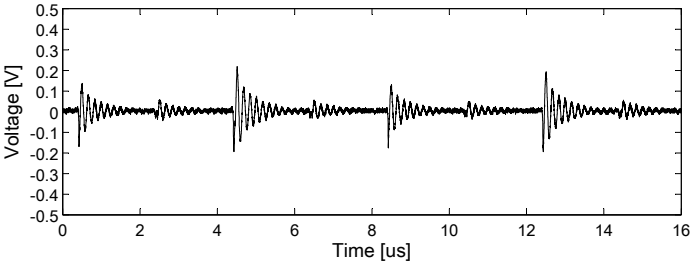

Fig. 4. The voltage waveform on the microprocessor power supply lines during the execution of MOVLW .0 instruction – program 1

Table 3. State of data bus before and after realization of the first machine cycle

	Program 1	Program 2	Program 3
The state of data bus before realization of the first machine cycle	0	3	240
The state of data bus after realization of the first machine cycle	0	12	15

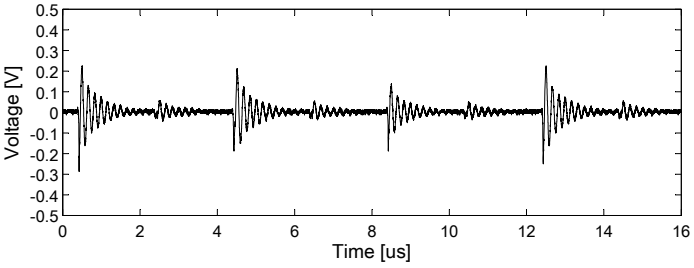

Fig. 5. The voltage waveform on the microprocessor power supply lines during the execution of MOVLW .12 instruction – program 2

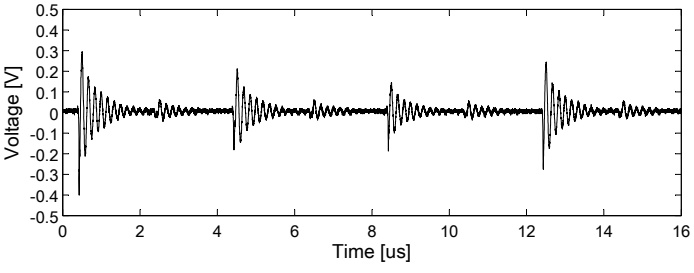

Fig. 6. The voltage waveform on the microprocessor power supply lines during the execution of MOVLW .15 instruction – program 3

voltage waveforms in the figures it can be seen the differences during the first and third machine cycle performance, whereas the voltage shapes for the second and fourth cycle are the same for all considered instructions. The rule of interaction on the first machine cycle can be explained as in the previous example, but it is not sufficient to explain the differences in the third machine cycle. Hence, it is necessary to examine the state of the microprocessor before and after the third machine cycle execution.

Before the third machine cycle of the tested instruction is realized, on the data bus is maintained a state that corresponds to instruction argument retrieved at the beginning of instruction cycle (the first machine cycle). Arithmetic Logic Unit operations are executed in the third machine cycle. In the considered example it is the summarizing operation. Next, the operation result is set on data bus, overwriting at the same time instruction argument, and then it is written into the accumulator W or to determined register in data memory (Table 4).

In order to explain the changes that occur in the voltage waveform during the first and the third machine cycle, it is helpful to use the parameter called Hamming distance (HD). In information theory, the Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. Put another way, it measures the minimum number of substitutions required to change one string into the other.

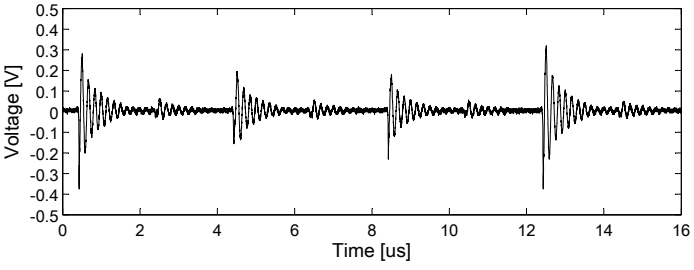

Fig. 7. The voltage waveform on the microprocessor power supply lines during the execution of ADDLW .63 instruction – program 4

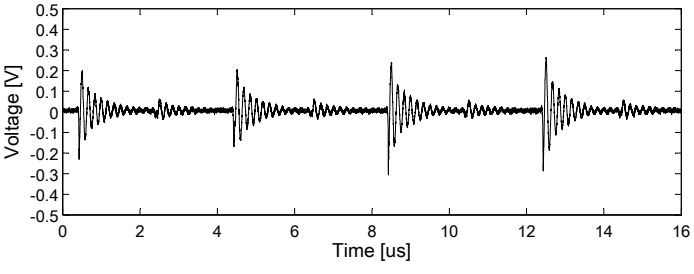

Fig. 8. The voltage waveform on the microprocessor power supply lines during the execution of ADDLW .12 instruction – program 5

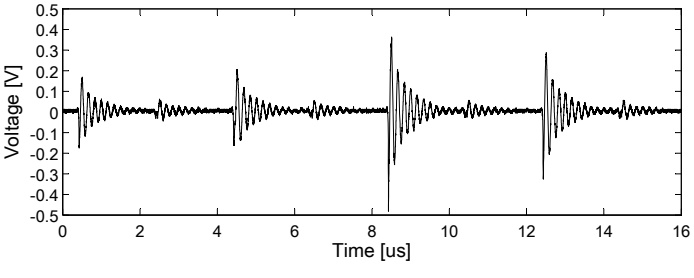

Fig. 9. The voltage waveform on the microprocessor power supply lines during the execution of ADDLW .85 instruction – program 6

Table 4. The state of data bus before and after realization of the third machine cycle

	Program 4	Program 5	Program 6
The state of data bus before realization of the third machine cycle	63	12	85
The state of data bus after realization of the third machine cycle	63	48	170

Table 1 illustrates test programmes for which the Hamming distance between the previous result and the argument of tested instruction (Table 3) was estimated from Equation (1), (2) and (3):

$$HD(0,0) = HD(00000000\text{b}, 00000000\text{b}) = 0 \quad (1)$$

$$HD(3,12) = HD(00000011\text{b}, 00001100\text{b}) = 4 \quad (2)$$

$$HD(240,15) = HD(11110000\text{b}, 00001111\text{b}) = 8\ . \quad (3)$$

As the equation results present, the larger number of positions with the difference between the instruction argument and data bus state, the higher voltage amplitude occurs during the first machine cycle. Table 2 presents test programmes for which the Hamming distance among the data buses state before and after realization of the third machine cycle (Table 4) was estimated from Equation (4), (5), and (6):

$$HD(63, 0+63) = HD(63,63) = HD(00111111b, 00111111b) = 0 \quad (4)$$

$$HD(12, 36+12) = HD(12,48) = HD(00001100b, 00110000b) = 4 \quad (5)$$

$$HD(85, 85+85) = HD(85,170) = HD(01010101b, 10101010b) = 8\ . \quad (6)$$

As in the previous case, the equation results suggest that together with the increase of Hamming distance, being the result of difference between instruction argument set on data bus in the first machine cycle, and the result of instruction operation, the voltage amplitude during the third machine cycle also increases.

5 Conclusion

As mentioned above, the main goal of the research is to determine a currently executed instruction on the basis of the emission of conducted disturbances on the power supply lines. However this subject matter requires a precise measurement and understanding of processes occurring inside the microprocessor during realization of the sequential instructions.

The presented results of the influence on parameters such as data bus state, instruction argument, the result of operation on the voltage waveform on the power supply lines of microprocessor, enable to understand the processes occurring during the realization of following instructions by microprocessor. In the technical specification of microprocessor units no information presented in this research is given, or it has only an elementary character. As the research result illustrate, not only instruction code, but also arguments on which the operation is executed, affect the supply voltage waveform during the realization of the instruction cycle.

The conducted emission of disturbances of power supply voltage (via supply lines) can be called compromising emanation, and its precise analysis may allow for reproducing the program code executing by microprocessor (reverse engineering). These issues will be taken into consideration in further authors research.

References

1. Piotrowski, R., Szczepański, S.: Input gate current uses to differential power analysis cryptographic device. XI International PhD Workshop. Wisła (2009)
2. Bendhia, S., Labussiere-Dorgan, C., Sicard, E., Tao, J.: Modeling the electromagnetic emission of a microcontroller using a single model. IEEE Transactions on Electromagnetic Compatibility (2008)
3. Maćkowski, M., Skoroniak, K.: Electromagnetic emission measurement of microprocessor units. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2009. CCIS, vol. 39, pp. 103–110. Springer, Heidelberg (2009)
4. Maćkowski, M., Skoroniak, K.: Instruction prediction in microprocessor unit based on power supply line. In: Kwiecień, A., Gaj, P., Stera, P. (eds.) CN 2010. CCIS, vol. 79, pp. 173–182. Springer, Heidelberg (2010)