DOI: 10.2507/27th.daaam.proceedings.031

RFID READER'S CONSTRUCTION IN TERMS OF ELECTROMAGNETIC SUSCEPTIBILITY

Martin Pospisilik[a], Zdenek Korytak[a], Peter Janku[a],
Rui Miguel Soares Silva[b] & Petr Neumann[a]

[a]*Faculty of Applied Informatics, Tomas Bata University, Nad Stranemi 4511, Zlin, Czech Republic*
[b]*Polytechnic Institute of Beja, Laboratory UbiNET, Rua Pedro Soares, Beja, Portugal*

This Publication has to be referred as: Pospisilik, M[artin]; Korytak, Z[denek]; Janku, P[eter]; Silva, R[ui] M[iguel Soares] & Neumann, P[etr] (2016). RFID Reader's Construction in Terms of Electromagnetic Susceptibility, Proceedings of the 27th DAAAM International Symposium, pp.0213-0218, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-08-2, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/27th.daaam.proceedings.031

Abstract

RFID technology has established itself in many sectors of human activity, including security and access systems. Just at this context, the demands on the hardware design in terms of its electromagnetic compatibility become critical. This paper provides a description of an immunity test against the electrostatic discharge according to the standard EN 61000-4-2 that was applied to an RFID reader which was primarily intended to be applied in access systems, employing the on-board recognition of the RFID tags. It was shown that such device can be endangered by the external electrostatic pulse; the findings described in this paper may be beneficial for the developers of the hardware for the RFID devices.

Keywords: Electrostatic discharge; RFID reader; Immunity test; ESD generator; Radiation pattern

1. Introduction

The issues on electrostatic discharges have become important deep in the nineteenth century when several paper mills had faced the accidents caused by ignition of the paper dust by spark discharges. Even earlier, the effects on spark discharges on gunpowder have also been known [3]. However, the problems of the electrostatic discharges have been comprehensively tackled since the first field-effect semiconductors begun to be employed. Nowadays the electrostatic discharge (ESD) protection is one of the most important issues at the electronic devices` development as the current semiconductors exhibit high sensitivity to the energy released during the discharge.

At present, testing of devices on the immunity to electrostatic discharges falls within the tests performed within the framework of electromagnetic compatibility (EMC) testing. In European Union, the set of immunity tests is prescribed by the standard EN 61000-4-1 and the conditions and criteria of testing on the ESD immunity are described by the standard EN 61000-4-2. This standard prescribes the criteria that must be fulfilled when the tested device is in operation as well [6] [7]. The device should be enclosed in its cover.

1.1 Electrostatic discharge

The local electrostatic discharge occurs between two surfaces provided there is a significant difference between their charges that are determined by the number of accumulated electrons. Lightning is probably the most dramatic effect of ESD, but in practice, even in much smaller discharges high powers are dissipated, which can result in unpleasant consequences. Although the typical energy released at one ESD reaches the order of mJ, due to very short discharge times (nanoseconds) the levels of voltage and current are destructive to most of the semiconductor devices. According to [2] the charge on the surface of a human body can reach up to 15 kV when walking or rubbing on clothing. A typical current waveform when ESD occurs is depicted in Fig. 1.

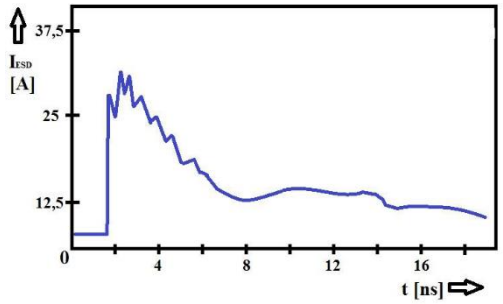

Fig. 1. Typical current waveform during the electrostatic discharge [2]

1.2 Standardization

As mentioned above, testing of any electronic device`s immunity against ESD falls among the issues on electromagnetic susceptibility. The generic standard EN 61000-6-1 defines functional criteria according to which the performance of the tested device can be objectified.

The ESD immunity test is defined by the standard EN 61000-4-2. By means of this standard, the voltage levels, pulse waveforms and the configuration of the experiment are prescribed as well as the steps of the experiment. As the source of energy, ESD simulators are used. According to the appropriate standards, the amount of energy released during the discharge is specified by the level of voltage on a capacitor, the capacitance of which is also defined by the standards. Therefore, the discharge voltage (4, 8 kV etc.) is specified instead of the amount of the electric charge. In addition, the dimensions and construction of the replaceable tips of the ESD generator are also specified by the appropriate standards.

The following test types can be applied:

- Discharge through the air gap
- Discharge through the direct contact
- Discharge through the coupling plane

2. Description of the experiment

The experiment was performed on the RFID reader that has been developed at the Tomas Bata University in Zlin. The goal of the experiment was to verify the level of the immunity of the RFID reader to the external electrostatic discharge. Moreover, the RFID´s reader antenna radiation pattern has been obtained by means of the near field probe. The details are provided in subchapters below.

2.1 Description of the reader

The block diagram of the RFID reader that was tested within this experiment is provided in Fig. 2. The construction is based on STM32F family microcontroller that has a direct connection to the RFID reader chip MFRC523. This chip provides a complete RFID interface that allows reading the tags of the appropriate access cards. The detailed description of the chip is provided in [4].

There are several ports available to establish the data transfer between the RFID reader's module and the connected data processing unit, because the RFID reader was intended to operate as a universal unit.

These ports are as follows:

- CAN bus based on the engine MCP 2550
- USB implemented directly on the processor's chip
- Direct parallel port driven by the microprocessor's I/O pins.

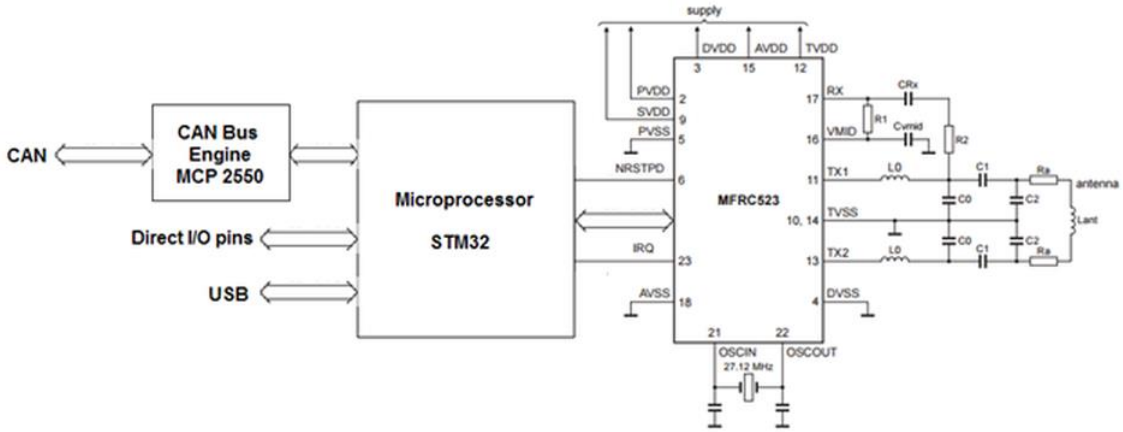

Fig. 2. Tested RFID reader's block diagram

For the purposes of the test, the following algorithm has been implemented to the reader's microcontroller: The RFID chip MFRC523 is periodically requested to detect and read the tag of the prospective RFID tag. Once the tag is detected and read, its unique number is compared to all numbers enlisted in the microcontroller's memory. When the tag is recognized and approved, a set of logical bits is send to the parallel port of the reader. This enables direct control of the connected device. For example, the door lock cen be opened directly by the RFID reader's unit. Moreover, there is a LED connected to one of the output pins to indicate the logical level at the appropriate output. Methods described in [8] have been applied in the unit's design.

2.2 Details of the experiment

The experiment has been performed inside the Laboratory of Electromagnetic compatibility of Tomas Bata University in Zlin in two steps. In the first step, the immunity of the reader's unit to the electrostatic discharge has been tested by means of the ESD generator ONYX 16 according to the standards EN 61000-6-1 and EN 61000-4-2. The test voltages were increased from the basic test level of 1 kV up to the levels prescribed by the abovementioned standards:

- ± 4 kV for a contact discharge
- ± 8 kV for a discharge through the air gap

All three test types, as described in the chapter 1.2 have been applied. The points of the RFID reader's unit that were hit by the ESD discharge were as follows:

- Input and output pins
- Status LED
- RFID antenna

Afterwards, another functional sample of the reader has been employed and its transmitting radiation pattern has been visualized by means of a close electrical field probe and the measuring receiver Rohde & Schwarz ESU 8. In this case, the intensity of the carrier frequency transmitted by the reader's antenna (13.56 MHz) has been mapped in the horizontal plane of the antenna in 70 different points and the results, processed by Maple software, has been visualised by means of the 3D graph. In both cases the tested reader was supplied from a laboratory power source.

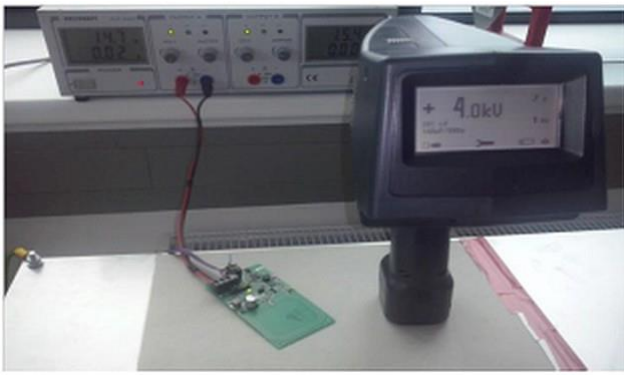

Fig. 3. The functional sample of the RFID reader and the ESD generator ONYX 16 [5]

Fig. 4. Measurement of the RFID reader's antenna radiation pattern

3. Results

The immunity test results are enlisted in Table 1. Different discharge types and voltage levels has been applied.

Point of ESD application	Charge voltage	Discharge type	Polarity	Result
I/O pins	4 kV	Contact	(+)	B
			(-)	B
LED (output state indicator)	4 kV	Contact	(+)	B
			(-)	B
RFID antenna	4 kV	Contact	(+)	C
			(-)	B
The whole reader through a vertical coupling plane	4 kV	Vertical coupling plane	(+)	A
			(-)	B
I/O pins	8 kV	Air gap	(+)	B
			(-)	B
LED (output state indicator)	8 kV	Air gap	(+)	B
			(-)	B
RFID antenna	8 kV	Air gap	(+)	B
			(-)	B

Table 3. Results of the immunity test

To fulfil all the requirements of the standard EN 61000-4-2, the worst achieved result should not be worse than B. As obvious from the Table 3, in one case this requirement has not been met. However, it must be considered, that the tested device was operated without the proper cover and the contact discharge was targeted directly to the receiver's antenna. This problem can be solved by enclosing the reader into a suitable cover.

After processing of the test the device has been checked for its proper operation and it has been found that no permanent damage occurred. Unfortunately, the test showed another problem that is not covered by the requirements of

the standard. When the device was influenced by the ESD, several logical 1 states occurred at the direct parallel bus. That means that there exists a real risk if the RFID reader is used directly to drive the actuators (for example the door lock), consisting in the fact that the attacker would bypass the authentication by giving the ESD shock to the RFID reader. On the other hand, this risk can be eliminated by using the modulated and/or encoded output peripherals as the CAN bus or USB. In this case, the RFID reader only gives the information on reading of the tag to another device that manages the actuators driving and the existence of accidental pulses on the communication bus cause no harm to the safety of the authentication system.

The results of the antenna`s radiation pattern are depicted in Fig. 5. From this figure it is obvious, that the antenna`s radiation pattern is symmetrical in terms of the space perpendicular to its z-axis. This determines the most critical direction of the interfering energy that could be sent by the aggressor in order to overload the RFID reader`s input.

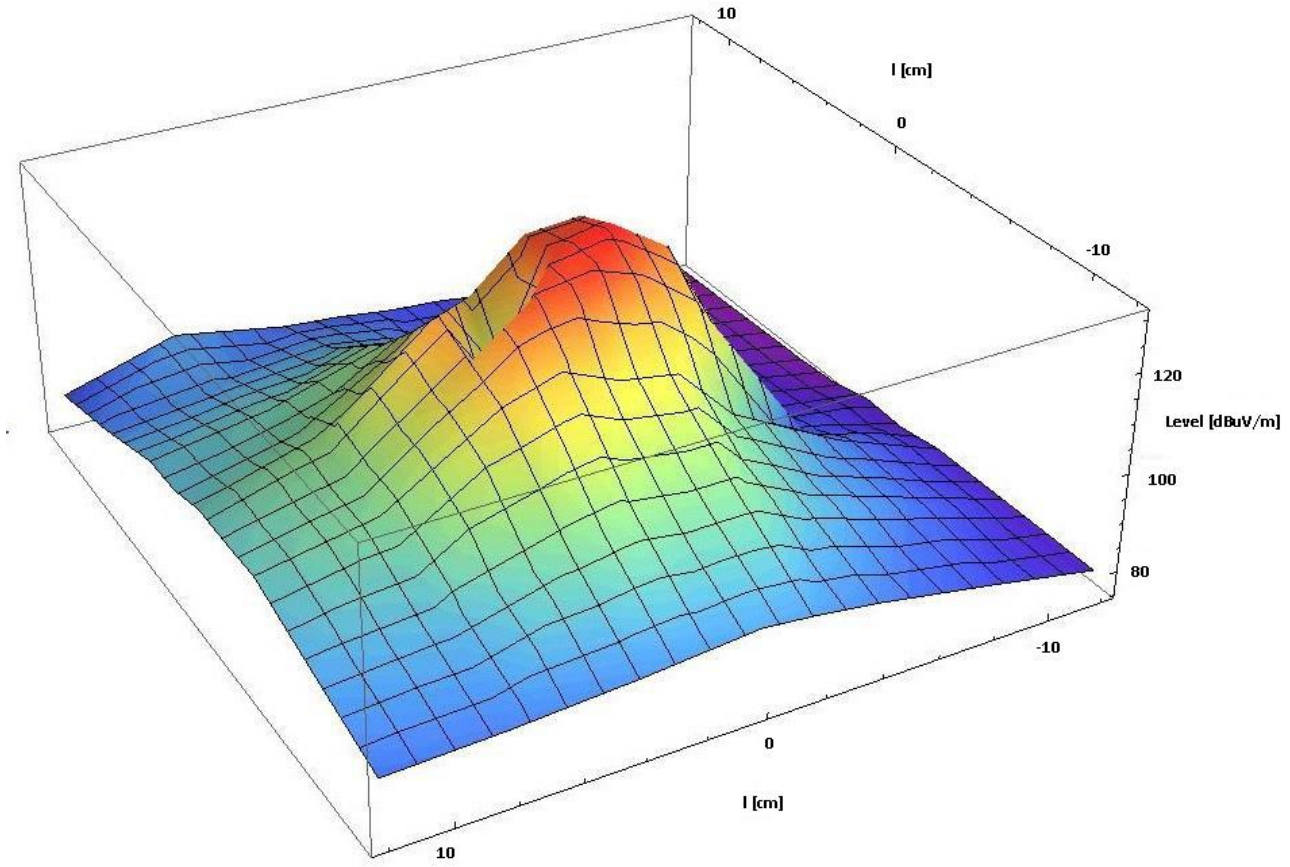

Fig. 5. RFID reader's antenna radiation pattern [5] (intensity vs. position)

4. Conclusions

In this paper a description of the ESD immunity test on a typical construction of the RFID reader is provided. The results of the test indicate, that if the RFID reader is intended to be used in a safety critical application, for example as a controller of the door lock, the phenomenon of the electrostatic discharge cannot be omitted, as the ESD can be generated deliberately as a kind of attack to the system. In this test a possibility of generating false positive signals at the output of the reader was confirmed. Therefore we recommend not to use the RFID reader directly to recognize the tags, but to process the information on the tags in the neighbourhood of the reader`s antenna by the remote device.

In addition, the radiation pattern of the RFID reader`s antenna has been obtained in order to check the antenna`s design and determine the direction of the external energy that will probably have the most harmful effect on the reader`s operation.

The hereby described experience with the tested device helped its manufacturer to improve its design in order to reach safer operation.

5. Acknowledgments

This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within The National Sustainability Programme Project No. LO1303 (MSMT-7778/2014) and also by The European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089.

6. References

[1] Svacina, J.. (2001). *Electromagnetic compatibility*. VUT Brno, Czech Republic.

[2] Horsky, P. (2014). Electrostatic discharge and testing of its inuence on integrated circuits. Online. URL: http://design.georgius.cz/sites/infocube/eem/horsky_eem081.pdf

[3] Poole, I. (2014). ESD Protection. Online. URL: https://radio-electronics.com

[4] MFRC523 (2016). Datasheet

[5] Korytak, Z. (2015). *Testing the Electromagnetic Susceptibility of Electrical Appliances*. Tomas Bata University in Zlin. Czech Republic

[6] Paul, C. R. (2006). *Introduction to electromagnetic kompatibility.* Wiley-Interscience. Hoboken.

[7] Vaculikova, P.; Vaculik, E. (1998). *Electromagnetic compatibility of electrotechnical systems*. BEN. Czech Republic

[8] Shah, R[ima]; Park, H[ong-Seok] & Lee, G[yu] B[ong] (2016). Design For Assembly: An approach to increase Design Efficiency of Electronics Home Appliance, Proceedings of the 26th DAAAM International Symposium, pp.0877-0882, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734- 07-5, ISSN 1726-9679, Vienna, Austria. DOI: 10.2507/26th.daaam.proceedings.122