Contactless Identification Card Immunity against a Current Pulse

Subjects: Automation & Control Systems

Contributor: Peter Vestenický, Marián Hruboš, Eduard Kolla

Contactless identification cards based on RFID technology are currently an integral part of many human activities in industry, transport, trade, etc. The most used cards are contactless cards operating at 13.56 MHz, according to the ISO/IEC 14443 standard, and using some version of the NXP Mifare chip.

Keywords: RFID ; Mifare ; current pulse ; voltage limiter ; approximation

1. Introduction

Contactless identification cards based on RFID technology [1] are currently an integral part of many human activities in industry, transport, trade, etc. The most used cards are contactless cards operating at 13.56 MHz, according to the ISO/IEC 14443 standard [2], and using some version of the NXP Mifare chip. Great emphasis is placed on the information security of the data stored in the chips of these cards. The immunity of these cards (or other forms of RFID transponders) to external electromagnetic fields which, in unfavourable cases, can destroy the identification chip by inducing a current pulse exceeding the safe value given by the chip manufacturer, is considered less often.

In practice, there are several cases in which RFID transponders can be destroyed by a current pulse induced from an adjacent linear conductor. **Figure 1** documents the use of RFID for marking underground cables and pipes. If these are metallic, they can conduct, e.g., part of the lightning current, endangering the transponder. The authors already have their own experience with such cases of transponder destruction. A similar situation can occur when embedding an RFID transponder in reinforced concrete in a bridge structure [3]. An example of an RFID transponder application (in this case, the UHF frequency band is used) in a railway vehicle chassis is given in [4], an environment with high traction currents. Other examples of the use of RFID technology in adverse environments with high currents are provided in [5] (RFID sensors for energy transmission lines), [6][7] (inductive power transfer for e-bikes equipped with RFID), and [8] (underground pipe monitoring). In [9], the design of a UHF RFID transponder for application in a strong electromagnetic field is described. Finally, for information security, the possibility of the targeted destruction of RFID cards with sensitive information (e.g., personal certificates) by a pulse in an external inductively coupled conductor (in this case, maybe a coil) is also interesting.

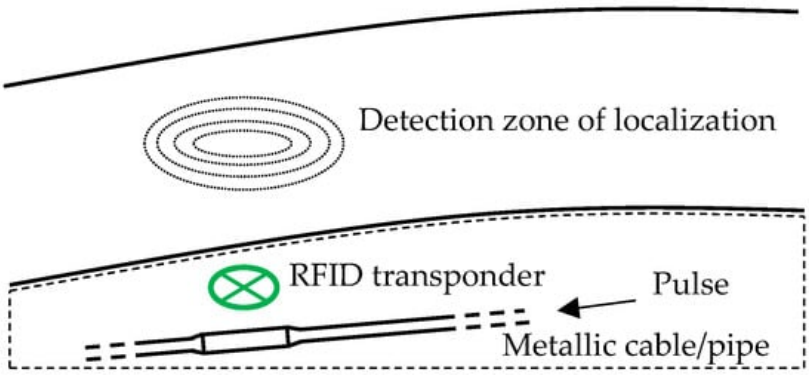

Figure 1. RFID transponder used for marking and locating the underground cables and pipes.

Each chip intended for incorporation into an RFID transponder, in addition to logic and memory elements, contains a voltage limiter that limits the maximum value of (alternating) voltage on the chip to approximately 4–8 V. The current–voltage characteristic of such a limiter looks like an anti-serially connected pair of Zener diodes characteristics, which causes significant nonlinear distortion of signals induced into the RFID transponder from reading devices. In the case of overcurrent induction (several tens of mA, [10]), the RFID transponder may be destroyed.

2. Evaluation of Contactless Identification Card Immunity against a Current Pulse in an Adjacent Conductor

The identification chips used in RFID transponders are principally nonlinear semiconductor components, usually manufactured using CMOS technology. The analysis and design of such chips are explained, e.g., in [11]. The nonlinear properties of identification chips for the UHF frequency band are described in [12][13][14]. The nonlinearity of HF RFID chips was documented in [15][16] by measuring the impedance of chips depending on the supply voltage within the allowed range according to the datasheets of the used chips. A powering circuit (rectifier and voltage regulator) for ISO/IEC 14443-compliant RFID chips based on CMOS technology was designed in [17]. However, this paper focuses on something other than the voltage limiter, which is mentioned only marginally. A detailed design of a voltage limiter for an RFID chip, specifically for the UHF frequency band, is provided in [18]. This design uses NMOS and PMOS transistors as a controlled load directly connected to the antenna terminals to limit the RF power in the chip. The analogue front-end for the 13.56 MHz transponder, including a powering circuit based on lateral MOS transistors, is described in [19][20]. The influence of a parallel-connected energy harvester on RFID transponder performance is modelled and measured in [21]. Other scientific works concerning power supply circuits of RFID chips are presented in [17][22][23][24][25][26][27].

The simplified mathematical model of the RFID chip used to calculate the current induced in the transponder assumes the approximation of the nonlinear current–voltage characteristic of the identification chip using suitable equations based on the mathematical description of the Zener diode. In general, sources [28][29] have dealt with the issue of semiconductor physics, while a more detailed analysis of models of semiconductor junctions applicable to Zener diodes can be found in [30][31][32].

Technical praxis is based on the regulations in the technical standard to evaluate the impact of overcurrent pulses caused by lightning [33]. This standard defines the time courses of voltage and current pulses, the simplified mathematical description of which can be found in the [34]. Electromagnetic compatibility tests of the proximity and vicinity identification cards and readers, e.g., intensity of magnetic field, sensitivity to electrostatic discharge, interferences etc., are described in the standards ISO/IEC 10373-6 [35] (for proximity devices, e.g., cards based on the NXP Mifare chip family) and ISO/IEC 10373-7 [36] (for vicinity devices, e.g., cards based on the NXP I-code chip family). These tests define the working conditions of the cards and readers that they must pass without damage.

RFID cards damaged during tests and measurements were measured using contactless means using a vector network analyser to calculate their state after the damage. For calculations, mutual relations between measured scattering parameters and the theoretical transfer function of measuring fixture were taken from [37][38][39][40].

The analyses of the electromagnetic field distribution and the standard working conditions of RFID transponders, necessary for their excitation, are presented in [41][42][43][44][45], and the electromagnetic field of the RFID reader is described in [46]. The possible destruction of RFID transponders and cards by a strong magnetic field with an intensity of more than 12 A/m is mentioned in [47]. The studies [48][49] deal with the tests of 125 kHz and 13.56 MHz RFID transponders in the strong magnetic field of MRI (magnetic resonance imaging) equipment. The paper [50] states that the damage of animal RFID transponders is almost certain when the animal crawls under a wirelessly charged vehicle where the magnetic field intensity is about 10 kA/m. There is also a patent [51] that describes the possibility of destroying an RFID tag using an electromagnetic pulse generator without further details.

The damage of the RFID card or transponder is one of the possible security (DOS—denial of service) attacks on the RFID system. The possibility of the DOS attack is mentioned in [52] and other security aspects of RFID systems are analysed in [53][54][55][56][57].

References

1. Neustupa, Z.; Danel, R.; Staša, P.; Beneš, F.; Švub, J. Ensuring the security of warehouse using automatic identification by RFID. In Proceedings of the ICCC 2015, 16th International Carpathian Control Conference, Szilvasvarad, Hungary, 27–30 May 2015; pp. 338–342, ISBN 978-147997370-5.
2. ISO/IEC 14443-1; Cards and Security Devices for Personal Identification—Contactless Proximity Objects—Part 1: Physical Characteristics. International Standard, 4th ed.; ISO: Geneva, Switzerland, 20 April 2018.
3. Strangfeld, C.; Stoppel, M.; Bartholmai, M.; Petrov, S.; Fakhouri, A. Embedded RFID Sensors for Concrete Bridge Structures. In Proceedings of the International Symposium Non-Destructive Testing in Civil Engineering (NDTCE 2015),

Berlin, Germany, 15–17 September 2015; Available online: https://www.ndt.net/?id=18255 (accessed on 8 November 2022).

4. Zhang, X.; Tentzeris, M. Applications of Fast-Moving RFID Tags in High-Speed Railway Systems. Int. J. Eng. Bus. Manag. 2011, 3, 27–31.
5. Tong, J.; He, Y.; Li, B.; Deng, F.; Wang, T. A Novel Design of Radio Frequency Energy Relays on Power Transmission Lines. Energies 2016, 9, 476.
6. Afonso, J.A.; Duarte, H.G.; Cardoso, L.A.L.; Monteiro, V.; Afonso, J.L. Wireless Communication and Management System for E-Bike Dynamic Inductive Power Transfer Lanes. Electronics 2020, 9, 1485.
7. Cardoso, L.A.L.; Comesaña Martinez, M.; Nogueiras Meléndez, A.A.; Afonso, J.L. Dynamic Inductive Power Transfer Lane Design for E-bikes. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2307–2312.
8. Vyas, R.; Tye, B. A Sequential RFID System for Robust Communication with Underground Carbon Steel Pipes in Oil and Gas Applications. Electronics 2019, 8, 1374.
9. Liu, X.; Song, R.; Fu, H.; Zhu, W.; Luo, K.; Xiao, Y.; Zhang, B.; Wang, S.; He, D. Anti-High-Power Microwave RFID Tag Based on Highly Thermal Conductive Graphene Films. Materials 2023, 16, 3370.
10. MF1S50YYX_V1: MIFARE Classic EV1 1K—Mainstream Contactless Smart Card IC for Fast and Easy Solution Development, Rev. 3.2, May 2018. Product Data Sheet, NXP Semiconductors. Available online: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf (accessed on 8 November 2022).
11. Paixão Cortes, F.; Schmidt, R.; Courcelle, L.; Pessatti, M. Low-frequency passive RFID systems implementation in CMOS technology: Design considerations and tradeoffs. In Proceedings of the SBCCI 2011, 24th Symposium on Integrated Circuits and Systems Design, João Pessoa, Brazil, 30 August–2 September 2011; pp. 1–4, ISBN 978-1-4503-0828-1.
12. Andia, G.; Duroc, Y.; Tedjini, S. Nonlinearities in Passive RFID: Third Harmonic Concept and Applications; ISTE Ltd.: London, UK; GB and John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2018; ISBN 978-1-78630-226-7.
13. Andia Vera, G.; Duroc, Y.; Tedjini, S. RFID Test Platform: Nonlinear Characterization. IEEE Trans. Instrum. Meas. 2014, 63, 2299–2305.
14. Seemann, K.; Hartmann, M.; Cilek, F.; Missoni, A.; Holweg, G.; Weigel, R. Nonlinear Behavioral Modeling of Passive RFID-Transponder-Frontends. In Proceedings of the 2007 IEEE Radio Frequency Integrated Circuits (RFIC) Symposium, Honolulu, HI, USA, 3–4 June 2007; pp. 479–484, ISBN 1-4244-0531-9.
15. Grosinger, J.; Deutschmann, B.J.B.; Zöscher, L.; Gadringer, M.; Amtmann, F. HF RFID Tag Chip Impedance Measurements. IEEE Trans. Instrum. Meas. 2022, 71, 2000911.
16. Gebhart, M.; Bruckbauer, J.; Gossar, M. Chip Impedance Characterization for Contactless Proximity Personal Cards. In Proceedings of the 2010 7th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2010), Newcastle Upon Tyne, UK, 21–23 July 2010; pp. 826–830.
17. Liu, D.; Wang, R.; Yao, K.; Zou, X.; Guo, L. Design and Implementation of a RF Powering Circuit for RFID Tags or Other Batteryless Embedded Devices. Sensors 2014, 14, 14839–14857.
18. Zöscher, L.; Grosinger, J.; Muehlmann, U.; Watzinger, H.; Bösch, W. RF voltage limiters for passive differential UHF RFID front-ends in a 40 nm CMOS technology. In Proceedings of the 2015 IEEE MTT-S International Microwave Symposium, Phoenix, AZ, USA, 17–22 May 2015; ISBN 978-1-4799-8275-2.
19. Moon-Ho, C.; Byung-Do, Y.; Nam-Soo, K.; Yeong-Seuk, K. A 13.56 MHz Radio Frequency Identification Transponder Analog Front End Using a Dynamically Enabled Digital Phase Locked Loop. Trans. Electr. Electron. Mater. 2010, 11, 20–24.
20. Dongsheng, L.; Huan, L.; Xuecheng, Z.; Liang, G.; Ke, Y.; Zilong, L. A High Sensitivity Analog Front-end Circuit for Semi-Passive HF RFID Tag Applied to Implantable Devices. IEEE Trans. Circuits Syst. I Regul. Pap. 2015, 62, 1991–2002.
21. Jankowski-Mihulowicz, P.; Kalita, W.; Skoczylas, M.; Weglarski, M. Modelling and Design of HF RFID Passive Transponders with Additional Energy Harvester. Int. J. Antennas Propag. 2013, 2013, 242840.
22. Bhattacharyya, M.; Gruenwald, W.; Jansen, D.; Reindl, L.; Aghassi-Hagmann, J. An Ultra-Low-Power RFID/NFC Frontend IC Using 0.18 µm CMOS Technology for Passive Tag Applications. Sensors 2018, 18, 1452.
23. Rueangsri, N.; Thanachayanont, A. High-voltage Analog Front-end Circuit for a Magnetically-coupled RFID Transponder. In Proceedings of the 2007 Asia-Pacific Conference on Communications, Bangkok, Thailand, 18–20 October 2007; pp. 335–338.

24. Zou, X.; Lin, H.; Lin, H.; Liu, D.; Guo, L.; Yao, K. Design and Implementation of an Analog Front-end Circuit for Semi-passive HF RFID tag. In Proceedings of the 2014 IEEE Radio Frequency Integrated Circuits Symposium, Tampa, FL, USA, 1–3 June 2014; pp. 389–392.
25. Wang, D.; Hu, J.; Tan, H.Z. A Highly Stable and Reliable 13.56-MHz RFID Tag IC for Contactless Payment. IEEE Trans. Ind. Electron. 2015, 62, 545–554.
26. Masui, S.; Ishii, E.; Iwawaki, T.; Sugawara, Y.; Sawada, K. A 13.56 MHz CMOS RF Identification Transponder Integrated Circuit with a Dedicated CPU. In Proceedings of the 1999 IEEE International Solid-State Circuits Conference. Digest of Technical Papers. ISSCC. First Edition (Cat. No.99CH36278), San Francisco, CA, USA, 17 February 1999; pp. 162–163.
27. Nabavi, S.; Bhadra, S. A 65-nm CMOS Self-Supplied Power Management System for Near-Field Wirelessly Powered Biomedical Devices. Electronics 2023, 12, 4622.
28. Streetman, B.G.; Banerjee, S.K. Solid State Electronic Devices, 6th ed.; PHI Learning Private Limited: New Delhi, India, 2009; ISBN 978-81-203-3020-7.
29. Colinge, J.P.; Colinge, C.A. Physics of Semiconductor Devices; Springer: New York, NY, USA, 2009; ISBN 978-1-4020-7018-1.
30. Hurkx, G.A.M.; De Graaff, H.C.; Kloosterman, W.J.; Knuvers, M.P.G. A New Analytical Diode Model Including Tunneling and Avalanche Breakdown. IEEE Trans. Electron Devices 1992, 39, 2090–2098.
31. Scholten, A.J.; Smit, G.D.J.; Durand, M.; Van Langevelde, R.; Klaassen, D.B.M. The Physical Background of JUNCAP2. IEEE Trans. Electron Devices 2006, 53, 2098–2107.
32. Yang, M.; McAndrew, C.C.; Chao, L.; Xia, K. Characterization and Modeling of Zener Diode Breakdown Voltage Mismatch. In Proceedings of the IEEE 32nd International Conference on Microelectronic Test Structures (ICMTS), Kita-Kyushu, Japan, 18–21 March 2019; pp. 149–153, ISBN 978-1-7281-1466-8.
33. IEC 61000-4-5; Electromagnetic Compatibility (EMC)—Part 4–5: Testing and Measurement Techniques—Surge Immunity Test. International Standard, Edition 3.0; International Electrotechnical Commission: Geneva, Switzerland, May 2014; ISBN 978-2-8322-1532-6.
34. Rous, Z. Overvoltage Protection of Telecommunication Lines and Equipment; NADAS: Prague, Czech Republic, 1981. (In Czech)
35. ISO/IEC 10373-6:2020; Cards and Security Devices for Personal Identification—Test Methods—Part 6: Contactless Proximity Objects. International Standard, 4th ed.; ISO: Geneva, Switzerland, 20 July 2020.
36. ISO/IEC 10373-7:2019; Cards and Security Devices for Personal Identification—Test Methods—Part 7: Contactless Vicinity Objects. International Standard, 3rd ed.; ISO: Geneva, Switzerland, 20 October 2019.
37. Castillo, J.A.; Flores-Troncoso, J.; Jáuregui, R.; Simón, J.; Alvarez-Flores, J.L. Signal Conditioning Stage in S-Band Communication Subsystem for CubeSat Applications. Electronics 2021, 10, 1627.
38. Avram, S.; Vasiu, R. Passive Power Line Communication Filter Design and Benchmarking Using Scattering Parameters. Appl. Sci. 2023, 13, 6821.
39. Zhao, J.; Wang, F.; Yu, H.; Zhang, S.; Wang, K.; Liu, C.; Wan, J.; Liang, X.; Yan, Y. Analysis and Design of a Wideband Low-Noise Amplifier with Bias and Parasitic Parameters Derived Wide Bandpass Matching Networks. Electronics 2022, 11, 633.
40. Lu, S.S.; Lin, Y.S.; Chiu, H.W.; Chen, Y.C.; Meng, C.C. The determination of S-parameters from the poles of voltage-gain transfer function for RF IC design. IEEE Trans. Circuits Syst. I 2005, 52, 191–199.
41. Fujisaki, K. Evaluation of Table Type Reader for 13.56 MHz RFID System Considering Distance Between Reader and Tag. In Advances in Network-Based Information Systems; Barolli, L., Kryvinska, N., Enokido, T., Takizawa, M., Eds.; NBiS 2018. Lecture Notes on Data Engineering and Communications Technologies; Springer: Cham, Switzerland, 2019; Volume 22.
42. Yoshigai, Y.; Fujisaki, K. Evaluation of 13.56 MHz RFID System Considering Tag Magnetic Field Intensity. In Advances in Networked-Based Information Systems; Barolli, L., Nishino, H., Enokido, T., Takizawa, M., Eds.; NBiS 2019. Advances in Intelligent Systems and Computing; Springer: Cham, Switzerland, 2020; Volume 1036.
43. Pesic, M.; Pachler, W.; Rampetzreiter, S.; Arthaber, H. Modeling and Design of Small, Passive, and Standard-compliant Proximity Coupling Transponders. In Proceedings of the 2020 IEEE International Conference on RFID, Orlando, FL, USA, 28 September–16 October 2020; pp. 1–7.
44. Blair, C.; Rautio, J.C. RFID Design Using EM Analysis, In Proceedings of the 2010 IEEE Long Island Systems, Applications and Technology Conference. Farmingdale, NY, USA, 7 May 2010; pp. 1–6.

45. Flores, J.L.M.; Srikant, S.S.; Sareen, B.; Vagga, A. Performance of RFID Tags in Near and Far Field. In Proceedings of the 2005 IEEE International Conference on Personal Wireless Communications, 2005—ICPWC 2005, New Delhi, India, 23–25 January 2005; pp. 353–357.
46. Zradziński, P. Modelling and Evaluating Electromagnetic Field Exposure in the Multiple-Source Scenario of Using IoT HF RFID Readers. Int. J. Environ. Res. Public Health 2022, 19, 3274.
47. Thevenon, P.H.; Savry, O.; Tedjini, S.; Malherbi-Martins, R. Attacks on the HF Physical Layer of Contactless and RFID Systems. In Current Trends and Challenges in RFID; InTech: Vienna, Austria, 20 July 2011.
48. Periyasamy, M.; Dhanasekaran, R. Assessment of safety and interference issues of radio frequency identification devices in 0.3 Tesla magnetic resonance imaging and computed tomography. Sci. World J. 2014, 2014, 735762.
49. Titterington, B.; Shellock, F.G. Evaluation of MRI issues for an access port with a radiofrequency identification (RFID) tag. Magn. Reson. Imaging 2013, 31, 1439–1444.
50. Mclean, J.; Sutton, R. The electromagnetic compatibility of wireless inductive automotive battery chargers and LF animal RFID tags. In Proceedings of the 2012 Asia-Pacific Symposium on Electromagnetic Compatibility, Singapore, 21–24 May 2012; pp. 921–7673.
51. System and Method for Detecting and Removing or Disabling RFID Tags. U.S. Patent US 20060152363A1, 13 July 2006. Available online: https://patents.google.com/patent/US20060152363A1/en (accessed on 8 November 2022).
52. Figueroa Lorenzo, S.; Añorga Benito, J.; García Cardarelli, P.; Alberdi Garaia, J.; Arrizabalaga Juaristi, S. A Comprehensive Review of RFID and Bluetooth Security: Practical Analysis. Technologies 2019, 7, 15.
53. Hutter, M.; Mangard, S.; Feldhofer, M. Power and EM Attacks on Passive RFID Devices. In Cryptographic Hardware and Embedded Systems—CHES 2007; Paillier, P., Verbauwhede, I., Eds.; CHES 2007. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727.
54. Hutter, M.; Schmidt, J.M.; Plos, T. RFID and Its Vulnerability to Faults. In Cryptographic Hardware and Embedded Systems—CHES 2008; Oswald, E., Rohatgi, P., Eds.; CHES 2008. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5154.
55. Hutter, M.; Schmidt, J.M.; Plos, T. Contact-based Fault Injections and Power Analysis on RFID Tags. In Proceedings of the 2009 European Conference on Circuit Theory and Design, Antalya, Turkey, 23–27 August 2009; pp. 409–412.
56. Fernández-Caramés, T.M.; Fraga-Lamas, P.; Suárez-Albela, M.; Castedo, L. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. Sensors 2017, 17, 28.
57. Musial, S.; Firlej, A.; Kubiak, I.; Dalecki, T. Electromagnetic Safety of Short-Range Radio Frequency Identification Systems. Electronics 2023, 12, 4391.