2nd URSI AT-RASC, Gran Canaria, 28 May – 1 June 2018

SATA interface in the process of electromagnetic infiltration

Rafał Przesmycki*(1), Marek Bugaj (1), and Marian Wnuk (1)
(1) Wojskowa Akademia Techniczna, ul. W. Urbanowicza 2, 00-908 Warszawa, http://www.wat.edu.pl

Abstract

The article concerns problems of electromagnetic compatibility and compromising emission that is the information security. The article focuses on the Serial Advanced Technology Attachment (SATA) interface for which extraneous signals used in the emission measurements are presented and the results of measurements of the compromising emission from the SATA interface are presented. In addition, the article discusses the laboratory stands for measuring compromising emission.

1. Introduction

Emission of electromagnetic field is a phenome-non constantly accompanying the passage of electric current which is, on the other hand, the basis of operation of all electronic and electric devices. Based on field changes it is possible to conclude about operation of devices being its source. What is more, properties of electromagnetic field permit its remote registration and analysis. The phenomenon of formation of electromagnetic waves carrying information about operation of electronic and electric devices is called com-promising emanation or corona. Since electric and electronic devices started to be used for information processing, often of confidential character, occurrence of compromising emission has acquired a particular importance [1].

Information security against electromagnetic permeability of devices and electromagnetic systems (IT) is of great importance. This problem increases with a higher and higher use of ICT devices for processing and trans-mitting information which should not fall into the wrong hands. It results from the fact that each electronic device is the source of undesirable (secondary) emission of electromagnetic energy induced in surrounding space and in all close conductors and metal structures [1].

When signals of undesirable emission are correlated with unclassified information, they can be used for reconstructing that information by intelligence services. The phenomenon of such undesirable emission is called compromising emission and its use by intelligence – penetration or electromagnetic infiltration. Undertakings which aim is to hinder system recognition on the basis of compromising emission are called information protection against electromagnetic penetration or emission safety [1].

Electromagnetic emissions with the feature of compromising emission can arise at any stage of processing of encoded information in the form of electric current courses. There is also no possibility to conduct tests of the source itself and the channel of information permeability. However such tests can be conducted in laboratory conditions in which examined devices are introduced into operation mode allowing to learn their infiltration susceptibility. In this article an example of such experiments has been presented. It seems that most suitable for illustrating the issue of electromagnetic information permeability are devices or their components which process information in serial way and the rule of encoding is uncomplicated and wellknown.

2. SATA Interface

Serial ATA (Serial Advanced Technology Attachment) is a computer bus interface that connects host bus adapters to mass storage devices such as hard disk drives, optical drives, and solid-state drives.

Revision 1.0a was released on January 7, 2003. First-generation SATA interfaces, now known as SATA 1.5 Gbit/s, communicate at a rate of 1.5 Gbit/s, and do not support Native Command Queuing (NCQ). Taking 8b/10b encoding overhead into account, they have an actual uncoded transfer rate of 1.2 Gbit/s (150 MB/s). The theoretical burst throughput of SATA 1.5 Gbit/s is similar to that of PATA/133, but newer SATA devices offer enhancements such as NCQ, which improve performance in a multitasking environment.

SATA revision 2.0 was released in April 2004, introducing Native Command Queuing (NCQ). It is backward compatible with SATA 1.5 Gbit/s.

Second-generation SATA interfaces run with a native transfer rate of 3.0 Gbit/s that, when accounted for the 8b/10b encoding scheme, equals to the maximum uncoded transfer rate of 2.4 Gbit/s (300 MB/s). The theoretical burst throughput of the SATA revision 2.0, which is also known as the SATA 3 Gbit/s, doubles the throughput of SATA revision 1.0.

Third-generation SATA interfaces run with a native transfer rate of 6.0 Gbit/s; taking 8b/10b encoding into account, the maximum uncoded transfer rate is 4.8 Gbit/s (600 MB/s). The theoretical burst throughput of SATA 6.0 Gbit/s is double that of SATA revision 2.0. It is backward compatible with SATA 3 Gbit/s.

In general, the enhancements are aimed at improving quality of service for video streaming and high-priority interrupts. In addition, the standard continues to support distances up to one meter. The newer speeds may require higher power consumption for supporting chips, though improved process technologies and power management techniques may mitigate this. The later specification can use existing SATA cables and connectors, though it was reported in 2008 that some OEMs were expected to upgrade host connectors for the higher speeds.

Figure 1. A seven-pin SATA data cable (left-angled version of the connector)

A special eSATA connector is specified for external devices, and an optionally implemented provision for clips to hold internal connectors firmly in place. SATA drives may be plugged into SAS controllers and communicate on the same physical cable as native SAS disks, but SATA controllers cannot handle SAS disks.
Female SATA ports (on motherboards for example) are for use with SATA data cables that have locks or clips to prevent accidental unplugging. Some SATA cables have right- or left-angled connectors to ease connection to circuit boards. The example of SATA connector is shown on Figure 1.

3. The laboratory stand for measuring compromising emission

In order to determine sources of compromising emission deriving from SATA interface it is necessary to estimate a contents degree of test signal intentionally generated by SATA interface (eSATA cable) in the signal received by measuring position as radiated or conducted compromising emission.
The laboratory stand for conducting tests of determining sources of compromising emission should make reception of generated test signal propagating as radiated or conducted compromising emission possible. In this article attention has been paid to radiated compromising emission. A sample system for testing forcing signals for compromising emission built on the basis of available on the market equipment has been presented in Figure 2.
For SATA interface as forcing for compromising emission used a requests a binary information sequences between PC and a hard disk connected using the interface and the eSATA cable. With the use of receiving antennas signal received by antenna gets through commutator which switches antennas to FSET 22 broadband receiver. In the receiver those signals are filtered and their conversion into lower frequency range takes place. Signal after detection is passed to VIDEO output in the receiver and then it is passed to input of external channel of oscilloscope on which there is a possibility of displaying received information in time domain [2, 3, 4].

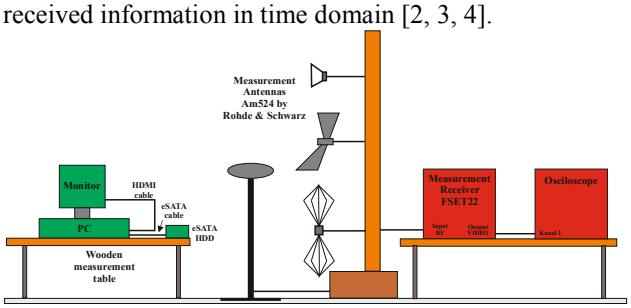

Figure 2. Block diagram of the laboratory stand for testing compromising emission

4. Measurements results

Ordinary observation of frequency spectrum obtained while the SATA interface transfer mode selected binary sequence can not answer as to the possibility of compromising emissions. It is not even possible to observe the beginning and end of data transfer. It is not possible to observe the phenomenon confirming the operation of the SATA interface in the form of data transmission.
During the emission tests of the SATA interface, you can only identify the work of the interface after connecting the device through this interface. It is not possible to observe the beginning and end of data transmission by comparing the time waveforms and its spectrum on transmission lines after the transmission is switched on and in the idle state (no forced data transmission on a given interface). In order to show the above phenomenon, the results of measurements for states are presented below, when the data transmission on the interface lines is forced and when such transmission is not forced.
The results of measurements in the form of frequency spectra for a pseudo-random binary sequence at a transmission speed of about 1 Gbit/s are shown in Figure 3, Figure 4, Figure 5 and Figure 6.

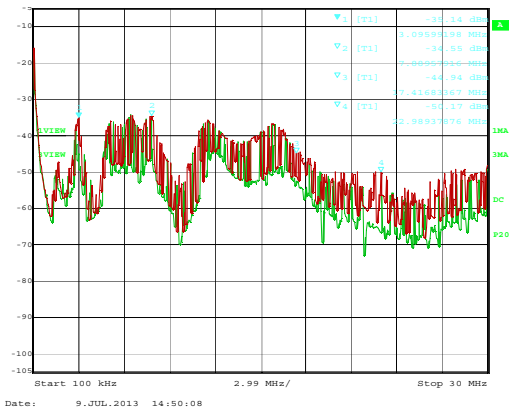

Figure 3. Radiated emission deriving from SATA interface while the transmission data is OFF (green color) and while transfer data is ON with 1 Gbit/s transmission speed (red color) in frequency range 100kHz – 30MHz

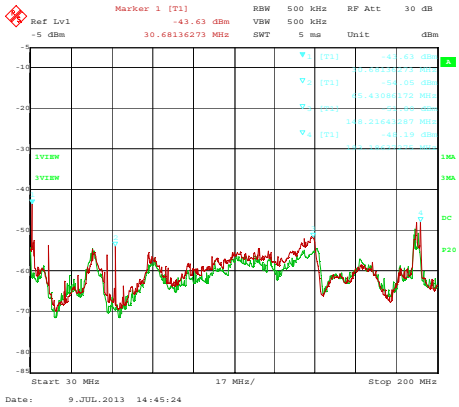

Figure 4. Radiated emission deriving from SATA interface while the transmission data is OFF (green color) and while transfer data is ON with 1 Gbit/s transmission speed (red color) in frequency range 30MHz – 200MHz

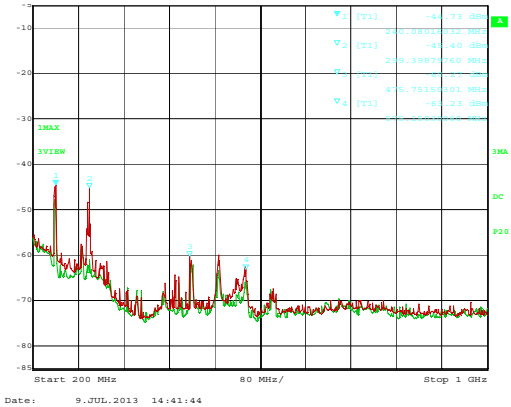

Figure 5. Radiated emission deriving from SATA interface while the transmission data is OFF (green color) and while transfer data is ON with 1 Gbit/s transmission speed (red color) in frequency range 200MHz – 1 GHz

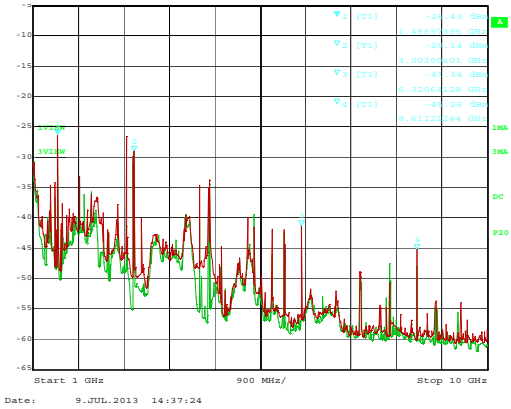

Figure 6. Radiated emission deriving from SATA interface while the transmission data is OFF (green color) and while transfer data is ON with 1 Gbit/s transmission speed (red color) in frequency range 1 GHz – 10 GHz

Very often evaluation of spectrum itself is insufficient due to difficulties resulting from rating of appearing signals at particular frequencies. Because of that it is necessary to use other methods consisting in the use of more advanced measuring devices. Anyway in most cases qualification of emissions occurs with the use of visual method. It should be remembered though that in doubtful cases or in such ones where visual assessment is impossible evaluation methods based on digital methods of processing of recorded signals are used.

Identification is a process or a result of processes of identifying a particular object with other object. It may include distinguishing common features, capturing similarities between a tested object and other objects of the same category, estimating values of observed parameters of a particular object. Using any methods of signal identification of compromising emission requires determination of distinctive features characteristic for model information signals and determination of a similarity degree of those features for analogous parameters of tested signals. On the basis of an analysis of radiated emission levels by SATA interface probable signal reception frequencies of compromising emission have been determined. To test whether radiated signals within that frequency range actually have the character of compromising emission, a series of recordings of those signals has been made with the use of digital oscilloscope and analyzed. The measurements were made when transferring data in the form of pseudo-random binary sequences between a PC and a hard disk connected using the interface and the eSATA cable. Examples of results are shown in Figure 7 and Figure 8.

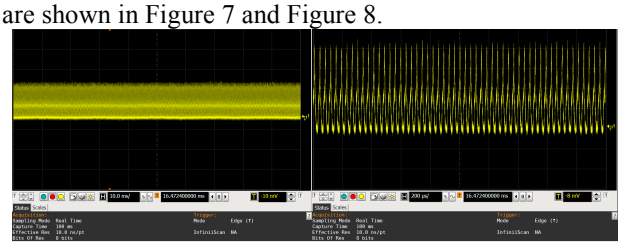

Figure 7. Oscillogram for the SATA interface during data transmission is OFF. The signal received by the antenna for f = 2,983 GHz given from the output VIDEO of the FSET22 receiver.

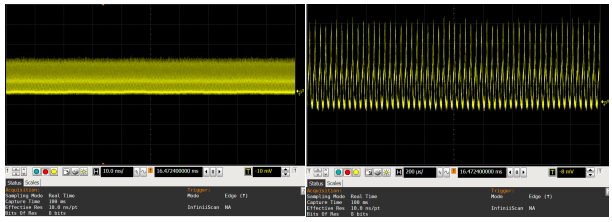

Figure 8. Oscillogram for the SATA interface during data transmission is ON. The signal received by the antenna for f = 2,983 GHz given from the output VIDEO of the FSET22 receiver.

In order to show the possibility of identifying the SATA interface, measurements were made during data transmission in the form of pseudo-random binary sequences between a PC and a hard disk connected using the interface and an eSATA cable using intermittent transmission. This transmission consisted in sending certain size files (binary sequences) between the PC and an external hard disk with specific forced interruptions in transmission. On the oscilloscope it was possible to observe the signal containing the data transmission and

after determining the FFT for this signal in the frequency spectrum one can see the bands spaced from each other by the frequency resulting from the duration of the data transmission interval. In order to show the above phenomenon, Figure 9, Figure 10 and Figure 11 show examples of measurement results for specific measurement conditions. During the measurements, data transmission was carried out, consisting in transferring a 100 MB file between the PC and an external hard disk with two specified transmission intervals - 30 ms and 100 ms. For a transmission interval of 30 ms in the frequency spectrum, we expect peaks spaced from each other by f = 33 Hz, while for a transmission gap equal to 100 ms in the frequency spectrum we expect peaks spaced from each other by f = 10 Hz. These values were estimated based on the dependence $f = 1/t_s$ where t_s is the duration of the interruption in transmission.

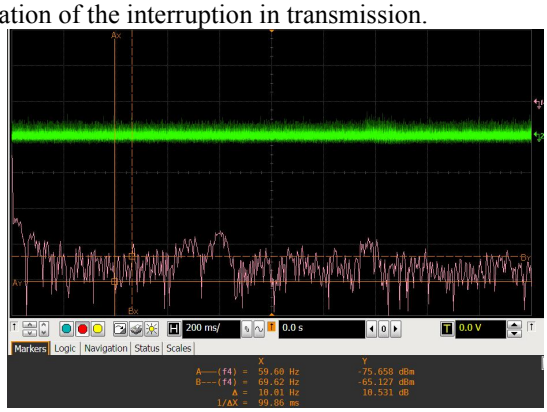

Figure 9. Oscillogram for the SATA interface during data transmission is OFF or ON. The signal received by the antenna for f = 4,52 GHz given from the output VIDEO of the FSET22 receiver.

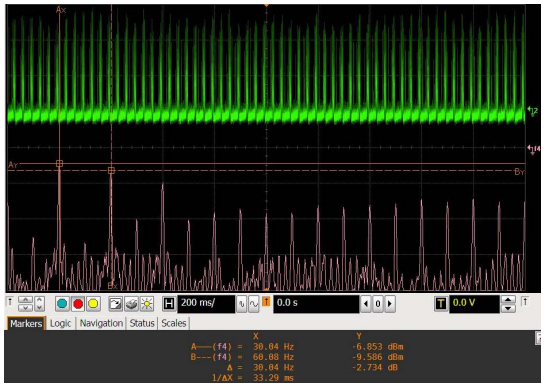

Figure 10. Oscillogram for SATA interface during data transmission is ON (transfer of file size 100 MB) with transmission intervals of 30 ms. The signal received by the antenna for f = 4,52 GHz given from the output VIDEO of the FSET22 receiver

5. Conclusions

From the time waveforms of radiated emission signals presented in the article for the SATA interface, it can be seen that these signals do not have a clear relationship with the content of transmitted binary sequences with a given transmission speed, and therefore they do not have the character of compromising emission signals. It is not possible to identify the content of the transmitted information in the time waveforms. However, it is possible to identify the operation of the SATA interface using intermittent transmission. Due to such transmission on the oscilloscope it was possible to observe the signal containing the data transmission and after determining the FFT for this signal in the frequency spectrum one can see the peaks separated from each other by the frequency resulting from the duration of the data transmission interval.

On the basis of the oscillograms obtained on the transmission lines of the interface and their spectrograms obtained during the use of intermittent transmission, it can be stated that: by choosing the right time of data transmission, the form of the signal waveform on the transmission lines of SATA interfaces can be shaped in such a way so that it can be easily identified.

Figure 11. Oscillogram for SATA interface during data transmission is ON (transfer of file size 100 MB) with transmission intervals of 100 ms. The signal received by the antenna for f = 4,52 GHz given from the output VIDEO of the FSET22 receiver

6. Literature

1. K. Grzesiak, I. Kubiak, S. Musiał, A. Przybysz, Elektromagnetyczne bezpieczeństwo informacji, Wydawca: WAT, Zegrze 2012,

2. Rafał Przesmycki Measurement and Analysis of Compromising Emanation for Laser Printer, Guangzhou, China, PIERS Proceedings 2014, str. 2661-2665, ISSN 1559-9450,

3. Przesmycki Rafal, Nowosielski Leszek – „USB 3.0 Interface in the Process of Electromagnetic Infiltration", Location: Shanghai, PEOPLES R CHINA Date: AUG 08-11, 2016, Book Series: Progress in Electromagnetics Research Symposium (PIERS), Pages: 1019-1023 Published: 2016, ISBN:978-1-5090-6093-1,

4. Przesmycki Rafal – „ Measurement and Analysis of Compromising Emanation for Laser Printer", Location: Guangzhou, PEOPLES R CHINA Date: AUG 25-28, 2014, Book Series: Progress in Electromagnetics Research Symposium Pages: 2661-2665 Published: 2014, ISBN:978-1-934142-28-8