Volume XXVI 2023
ISSUE no.2
MBNA Publishing House Constanta 2023

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

TEMPEST vs Commercial Equipment

To cite this article: C. Păiuș, C. Răcuciu, R. Moinescu and O. Bercea, Scientific Bulletin of Naval Academy, Vol. XXVI 2023, pg. 149-156.

Submitted: 16.04.2023
Revised: 25.06.2023
Accepted: 20.12.2023

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-23-I2-018

TEMPEST vs Commercial Equipment

Cătălin PĂIUȘ[1], Ciprian RĂCUCIU[1], Radu MOINESCU[1], Octavian BERCEA[2],
[1]Military Technical Academy "Ferdinand I" – Systems Engineering for Defense and Security
[2]Petroleum-Gas University of Ploiești – Automation and Applied Informatics

Abstract. When one thinks about TEMPEST and compromising electromagnetic emissions, he might think that everything is possible only with the help of sophisticated and expensive dedicated field equipment.
Due to the technological evolution and the appearance of small and affordable broadband receivers with notable capabilities, the analysis of compromising electromagnetic emissions has become much easier to achieve but also led to an increased risk in terms of information security.

Key words: *Receiver, equipment, compromising emissions, risk, TEMPEST.*

1. TEMPEST - CONCEPT

Since as early as the 1960's, it has been known by military organizations that all electrically powered apparatus generates electromagnetic radiation that not only disrupts radio reception, but also reveals information about the processed data, if it is a communication equipment. Known as compromising emanations or TEMPEST radiation, a code word for a US government program aimed at investigating the problem, unintentional electromagnetic transmission of data has been a significant problem in sensitive computer applications.

The term "TEMPEST" is commonly used throughout the entire field of emission safety or emanation security (EMSEC). TEMPEST is not an acronym and has no particular significance but is often translated as telecommunication electronic material that is protected from eminent spurious transmissions.

The term "TEMPEST" has been coined as a code name for the operation of the National Security Agency to protect electronic communications equipment from potential eavesdroppers and, conversely, the ability to intercept and interpret such signals from other sources.

2. COMMERCIAL EQUIPMENT - RECEIVER

Receivers are devices made up of a set of specialized electronic circuit blocks that have the purpose of receiving radio signals, processing them through selection, amplification, decoding, demodulation and conversion, all to reproduce the transmitted information generated by a source. The improvements of electronic devices and the technology used to build the electronic circuits has led to the evolution and diversification of the constructive types of radio receivers.

The internal structure of these receivers did not undergo major changes in terms of internal functioning organization, referring to the fact that they are structured by functional blocks with unique and well-established role.

Aside from the classical type of radio receivers that are designed to perform specific functions, like the radio receiver in your vehicle, the Wi-Fi module from inside of your computer, that have hardware designed and implemented to function within a certain array of parameters and are dedicated

for a distinct application, the evolution led to the emergence of relatively new types of radios for which some of the hardware blocks have been replaced by software code and can perform a large variety of functions from decoding commercial radio station broadcasts to receiving digitally encrypted data transmission.

These new types of receivers are known as SDRs (Software Defined Radio), which use software modules to process radio signals, consist of dedicated signal analysis software that run on a computer like hardware equipment or an embedded system with software and hardware specialized to digitize, filter and demodulate radio signals. SDRs can also be programmed to implement advanced signal processing techniques such as adaptive filtering, digital signal processing and error correction coding.

3. CAPTURED ELECTROMAGNETIC EMISSIONS

To demonstrate the capabilities of the new receivers that have software components, the following equipment is needed: a test equipment, a receiver based on SDR and a directive antenna.

By capturing the electromagnetic emissions, generated involuntarily by a system, with the help of equipment that can be purchased at a reduced price, the risk to which any system that is not designed with TEMPEST protection measures in mind, leaves it exposed and will be demonstrated in the next paragraphs.

Only the identification of the electromagnetic emissions generated by the system's components of interest, in a normal operating mode, and the evaluation from the point of view of the danger of these leaked emissions which can be captured with such an accessible equipment, will be followed.

In the following example, the equipment under test is a laptop computer.

With the help of a Signal Hound BB60C spectrum analyzer SDR, we will attempt to capture the emissions that the computer involuntarily generates during operation. These emissions will be classified as compromising or non-compromising electromagnetic emissions.

The criteria by which they are being classified consider the energy level of the emission and the component that involuntarily generates this emission. For a correct overview, the measurements will be conducted inside the Faraday chamber for the first phase of the test.

The laptop (Lenovo M5400) used in this experiment has the following configuration:

- Central processing unit: Intel® Core™ i5-4200M;
- Graphics processing unit: NVIDIA® GeForce® GT740M with 2GB graphics memory;
- Memory: 4.0 GB DDR3L – 1600 MHz;
- Operating System: Windows 10 Home;
- Display / Resolution: 15.6" HD display (1366 x 768), 16:9 widescreen.

Figure 1. Lenovo M5400

The BB60C spectrum analyzer used for the measurements has the following technical specifications:

Figure 2. Signal Hound BB60C

- RF frequency range from 9 kHz to 6 GHz;
- Up to 24 GHz/sec sweep speed (≥10 kHz RBW);
- Wide Dynamic Range from -158 dBm to +10 dBm;
- Resolution bandwidths available from 10 Hz to 10 MHz;
- Digitized IF Data at 80 million samples per second;
- 27 MHz instantaneous bandwidth.

To perform the measurements from a TEMPEST point of view, some known unintentional emissions are chosen, that is, the emissions generated by the computer's display panel. Thus, the component of the equipment is analyzed from a constructive point of view, the way it communicates with the adjoining components and the way presents the information.

The laptop's display panel has the following specifications:

- Panel Type: a-Si TFT-LCD, LCM;
- Resolution: 1366(RGB)×768, WXGA 100PPI;
- Pixel Format: RGB vertical stripe;
- Active Area: 344.232(W)×193.536(H) mm;
- Bezel Opening: 349.58(W)×198.29(H) mm;
- Outline Size: 359.3(W)×209.5(H) ×5.5(D) mm;
- Contrast Ratio: 650:1;
- Display Colors: 262K;
- Lamp Type: 9S6P WLED;
- Frequency: 60Hz;
- Signal Interface: LVDS (1 ch, 6-bit), 40 pins connector;
- Input Voltage: 3.3V.

Choosing the right antenna

In order to correctly choose the antenna that captures the involuntarily generated electromagnetic emissions, it is necessary to determine the frequencies on which the test equipment's display panel generates electromagnetic emissions.

The clock frequency of the video signal during display operation is calculated using the formula:

$$F_d = t_p \cdot t_l \cdot r_r \quad (1)$$

where:

F_d – video signal clock frequency;
t_p – total number of pixels per line;
t_l – total number of lines;
r_r – refresh rate.

For the emissions generated by the display panel the use of a high gain directional antenna is necessary so that the electromagnetic emission could be captured whole and the information carried recoverable with ease. Thus, for the intent, the chosen antenna is a log-periodic antenna (ETS-lindgren, model 3148) with the following characteristics:

Frequency range: 200 MHz – 2 GHz;

VSWR: 1.2:1 (average) / 2.0:1 (max.);

Polarization: Lineary;

The antenna factor parameter data is shown in figure 3:

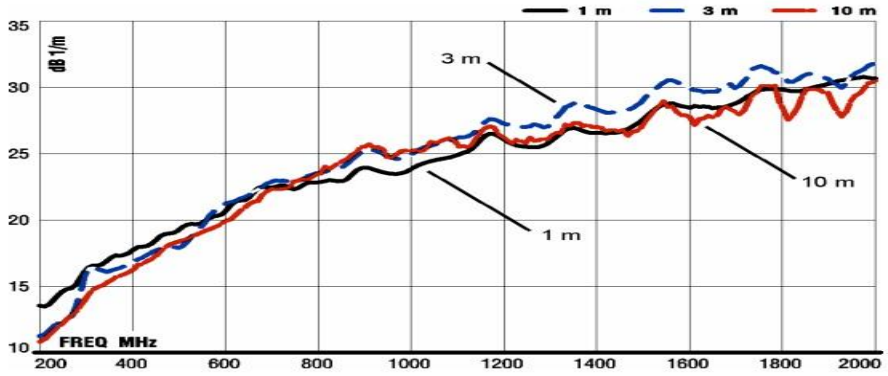

Figure 3. Antenna Factor

The electric field strength, in db[V/m], for the measured emissions, is obtained from the following formula:

$$E(dBV/m) = V(dBV) + AF(dB1/m) + \alpha(dB) \quad (2)$$

Where:

$V -$ the receiver voltage reading;

$AF -$ antenna factor;

$\alpha -$ cable loss in dB, if cable losses are non $-$ negligible.

This antenna has a good gain (see figure 4), a characteristic required for measurements.

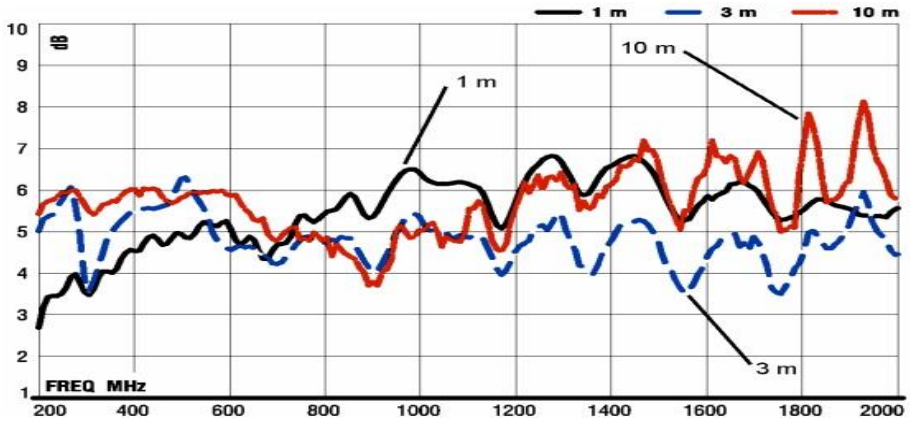

Figure 4. Antenna Gain

The test setup inside the Faraday chamber (figure 5) comprises the following components:

- log-periodic antenna
- laptop
- radio frequency cables.

Figure 5. Test setup

To begin with, it is necessary to measure the ambient noise level inside the Faraday chamber. This measurement, made in the 200 MHz - 2 GHz band, in radio silence, with all electronics inside the chamber powered off, is called reference measurement. Figure 6 reveals the ambient noise level measured with the BB60C receiver and presented with the Spike application.

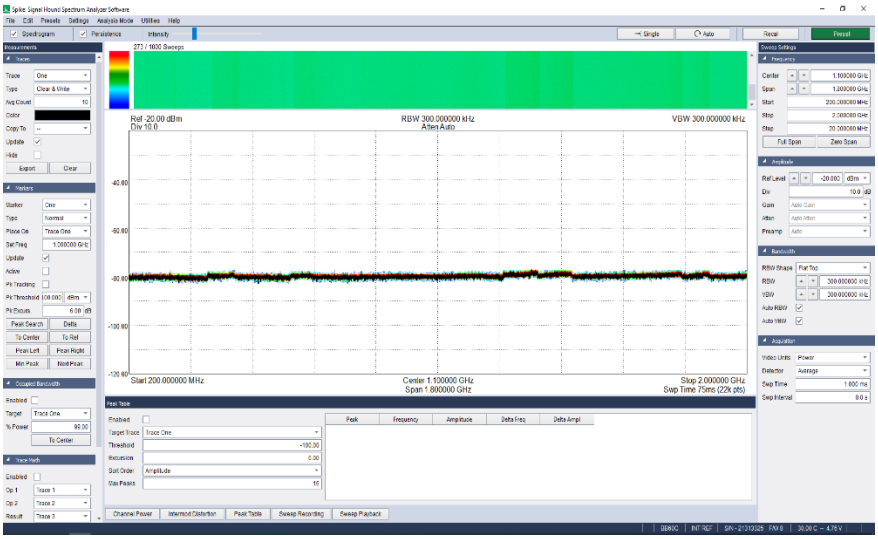

Figure 6. Ambient noise level

After the measurement of the ambient noise level, a second measurement is performed, this time with the laptop under test powered on. Figure 7 unveils the state and level of the electromagnetic

spectrum when the laptop is turned on and operates in a normal mode. The differences between the first and the second measurements represent the electromagnetic emissions generated involuntarily by the laptop.

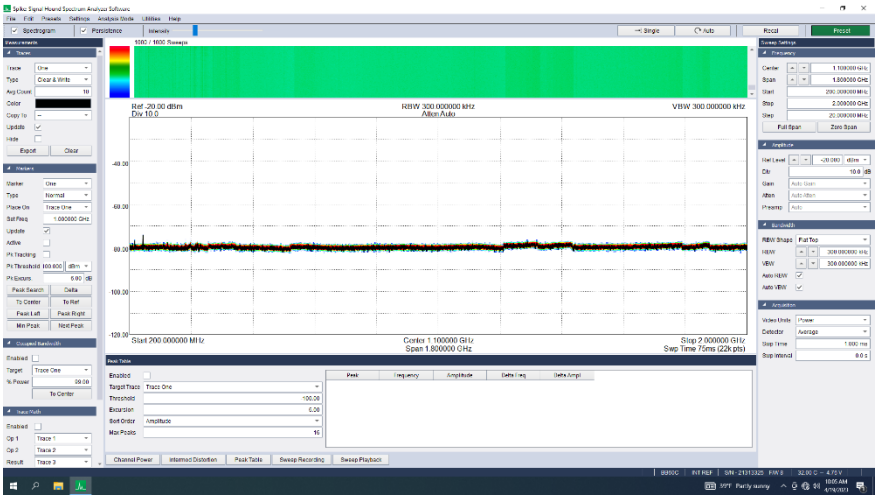

Figure 7. Unintentionally generated emissions

The conspicuous signal that differentiates the second measurement from the reference measurement is located in the 225 MHz - 275 MHz frequency area. We will be focusing and enlarge that specific area for a better view of the electromagnetic spectrum. Clearly, the computer's display electromagnetic frequency signal is located at 240 MHz.

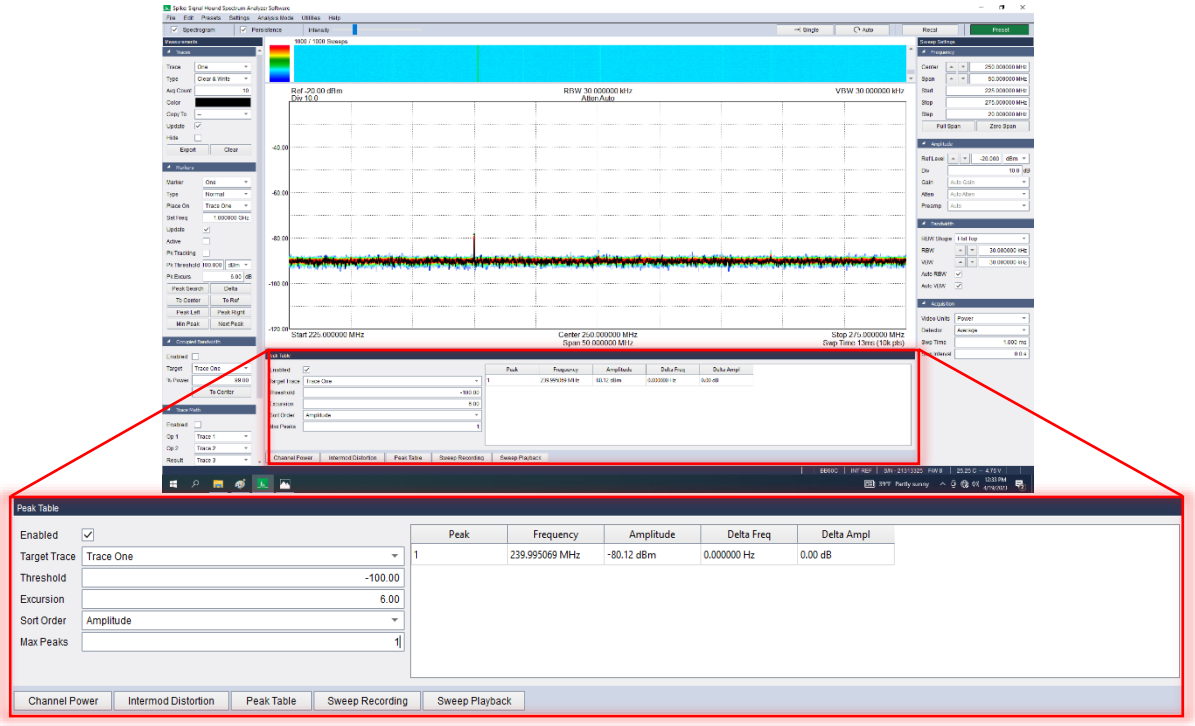

Figure 8. Magnification on the emission zone

To demonstrate the usefulness of this type of receiver and its capabilities regarding the analysis of electromagnetic emissions generated involuntarily, more precisely the risk it represents for the security of emissions (EMSEC), the following measurement will be performed outside of the Faraday chamber to determine if it is possible to identify this 240 MHz emission, in open space, in the presence of multiple disturbances across the spectrum and even more, incoming at harm of variable signals strengths. These disturbances may hinder the capability to identify, capture or analyze the display panel electromagnetic signal by flooding, overpowering or interfering with it.

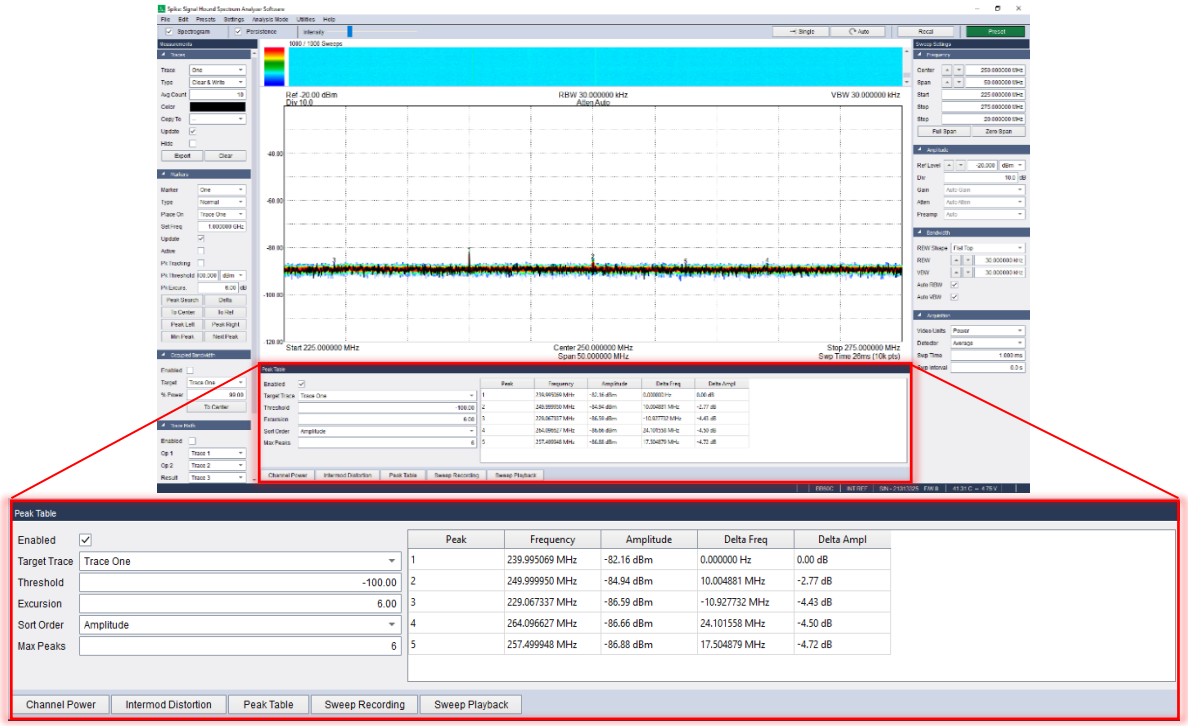

Figure 9. Outside measurement

4. CONCLUSION

The process of capturing electromagnetic emissions generated involuntarily by electronic equipment, with various inconspicuous signal frequencies, has recently become much more attainable on the strength of the technological evolution that we are facing, so that any person, by purchasing some commercial equipment, can perform such task.

Capturing the electromagnetic emissions generated by the equipment requires the use of a directional antenna, a commercial SDR receiver and a laptop computer to interpret the results.

In a space where the level of the ambient electromagnetic field is not high, the capture of unintentionally generated electromagnetic emissions becomes, on the benefit of technological evolution, more and more accessible for most people.

5. REFERENCES

[1] https://tomverbeure.github.io/video_timings_calculator
[2] https://app.box.com/s/vcocw3z73ta09txiskj7cnk6289j356b
[3] https://signalhound.com/support/compare-our-spectrum-analyzers-and-signal-generators/
[4] https://www.ni.com/ro-ro/innovations/white-papers/17/software-defined-radio--past--present--and-future.html
[5] https://www.lenovo.com/lt/lt/laptops/lenovo/m-series/m5400/?orgRef=https%253A%252F%252Fwww.google.com%252F
[6] https://www.theemcshop.com/log-periodic-dipole-array-antenna/1420-ets-lindgren-3148.html
[7] https://www.ets-lindgren.com/get-manuals/3148B(1).pdf
[8] file:///C:/Users/vizitator/Downloads/Lucrarea-1-Semnale-periodice.pdf
[9] https://www.afahc.ro/ro/facultate/cursuri/ccg/MSE/C05%20-%20Semnale%20periodice.pdf
[10] https://www.techopedia.com/definition/25856/emission-security-emsec
[11] ST 296:2012 - SMPTE Standard - 1280 × 720 Progressive Image 4:2:2 and 4:4:4 Sample Structure — Analog and Digital Representation and Analog Interface