TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.2, February 2014, pp. 866 ~ 871
DOI: http://dx.doi.org/10.11591/telkomnika.v12i2.4006

The Designing of TEMPEST Security Testing Model

Liu Jinming*, Mao Jian, Zhang Jiemin, Li Yongmei
Computer Engineering College, JiMei University (JMU)
No.183 Yinjiang Rd, Jimei, Xiamen, Fujian, China, Ph./Fax: +86-592-6182451/6181601
*Corresponding author, e-mail: liujinming@jmu.edu.cn

Abstract

Computer and other digital electronic equipments can emit unintentional electromagnetic signals in the state of information processing. The compromising electromagnetic emanations allow eavesdroppers to reconstruct processed data at a distance that threatening the information security. As result all equipments handling confidential information do need TEMPEST security testing. This paper attempts to design a mathematical model for TEMPEST testing that will facilitate the analysis of the key factors in TEMPEST testing and standard revising.

Keywords*: electromagnetic emanation, data security, TEMPEST, testing, model design*

1. Introduction

TEMPEST testing is to acquire the electromagnetic emanations such as emission intensity, parasitic leakage, signal bandwidth, characteristics in time domain and frequency domain, etc, by special equipments then rating security level [1, 2]. The purpose of TEMPEST testing is to check the information equipment whether there is electromagnetic information leakage risk or not, and assess the equipment's security level then limit its working zone [3-5]. To ensure accuracy of testing results, it is need to select correct methods, testing equipments and environment suitable for different EUT.

2. Mathematical Description of the Key Factors

There are two methods in testing compromising electromagnetic emanations of the digital equipment, such as frequency-domain method and time-domain method [6]. The time-domain measurement can get waveform in time domain and grasp its characteristic parameters by analyzing periodic signals. The frequency-domain method can get the radiation spectrum and frequency range, radiation intensity etc.

In the testing, the characteristics of EUT, accuracy requirements, test equipment, test environment and so on must be put into consider. The test item include emission intensity, pulse width, rising time, falling time, frequency, duty ratio, signal bandwidth, pulse repetition patterns, etc, to find if it contains useful information [7-10].

The actual test results are mainly affected by the antenna system, test environment, test equipment and analysis methods. For the model description's convenience, these factors are expressed in mathematical symbols.

2.1. Antenna System-T

Antenna system refers to the receiving antenna selection, antenna counterpoise lapping method, antenna positioning, and antenna test system checking method. The receiving antenna can turn the electromagnetic energy into voltage value and make the following measurement possible. The receiving antenna can be classified into two types such as magnetic field antenna and electric filed antenna according to different application. The magnetic field antenna is used to receive the magnetic field of the space electromagnetic environment or emanated from the EUT. The electric field antenna is used to receive the electric field. Magnetic antenna for receiving magnetic field emanated from the EUT or magnetic field of the electromagnetic environment. Which type of antenna is selected that according to the need of test items. Each

Received June 24, 2013; Revised August 15, 2013; Accepted September 13, 2013

type has different characteristics and receiving ability. When a single antenna can not meet the requirements, it's need to combine several receiving unit.

The comprehensive performance of antenna system is described as attribution T just representing the ability of capturing weak electromagnetic signal in space. The value of T is the weighted average of numerous performance figures, such as the field sensitivity, limit test frequency, etc.

2.2. Testing Environment-E

The electromagnetic emanations testing environment is needed to ensure the required measurement sensitivity and accuracy. It is generally required that the environment noise must be 10dB lower than the minimum level of EUT's radiation, the ground conducted emissions electromagnetic noise and environment noise should be at least 6dB lower than the permissible limit values when the EUT is powered off. There're several testing environments available such as outdoor open ground, shielded room, anechoic chamber, transverse electromagnetic transmission chamber (TEM chamber), gigahertz transverse electromagnetic cell (GTEM cell). But the widely used digital equipment makes it difficult to find the open test field; therefore, anechoic chamber is often used to replace the outdoor open field.

The comprehensive performance of testing environment is described as attribution E just representing the ability of reducing or eliminating outside interference to ensure the sensitivity and accuracy of measurement. The value of E is the weighted average of numerous performance figures.

2.3. Testing Equipment-C

There are many types of testing equipment, such as analysis instrument, frequency measuring instrument, radio character measuring instrument and auxiliary instrument. Preliminary amplifier, TEMPEST test receiver, digital oscilloscope, spectrum analyzer and virtual instrument are commonly used.

The comprehensive performance of testing equipment is described as attribution C just representing the ability of processing antenna induction signal quickly, such as attenuating, filtering, amplification, quantifying, coding, displaying and storing. The value of C is the weighted average of numerous performance figures of the testing equipment.

2.4. Red Signal Analysis Method-M

The purpose of TEMPEST testing is to prevent electromagnetic emanation--namely guarding red signal against electromagnetic radiation, make it difficult to intercept and reproduce the electromagnetic information-and don't care about the useless information emanation. TEMPEST is based on EMC technology so they have some connection, but they are not the same. The concept of red/black is a key word in TEMPEST, and that is distinct from EMC.

The comprehensive performance of red signal analysis methods is described as attribution M just representing the ability of extracting red signal from the testing equipment output. It is hard to assess the efficiency of those red signal analysis methods. The value of M here is defined as weighted average of the maturity of numerous analysis methods.

3. Mathematical Model of Testing

The test result of EUT can be expressed as:

$$X = \varphi(T, E, C, M)\big|R \tag{1}$$

X in (1) is the emission result tested from EUT, and R is the electromagnetic emanations of EUT, T is the comprehensive performance of antenna system, E is the comprehensive performance of testing environment, C is the comprehensive performance of testing equipment, M is the comprehensive performance of red signal analysis method, the last four parameters are already defined in the above section.

Equation (1) expresses that electromagnetic emanation testing is under the condition of one given EUT, and the measurement result X is determined by T/E/C/M, that is to say the

accuracy of the result is primarily affected by the attributes of antenna system, testing environment, testing equipments and red signal analysis methods.

The electromagnetic emanations R of EUT under a certain working state is determined by the equipment production technology and power voltage, then the objective R is a fixed value. The purpose of testing is to make the testing result X as far as possible close to R, as Equation (2) expressed.

$$\mathrm{R} = MAX(X) \tag{2}$$

For antenna system, the enhancement of antenna sensitivity depends primarily on the antenna structure, manufacturing technique, material used and so on. With the development of the antenna theory and material, and the improvement of manufacturing technique, the comprehensive performance of antenna system will improve continuously. Figure 1 shows the development of antenna performance, solid line represents the actual performance development, dot line represents the trend of performance development. It is clear that the value T of antenna performance is approximately a linear increasing function of time.

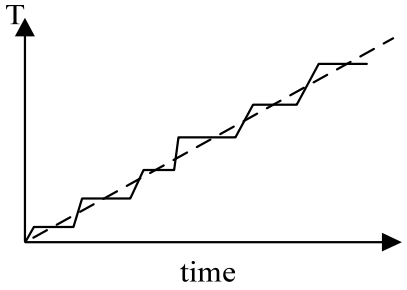

Figure 1. Development of Antenna Performance

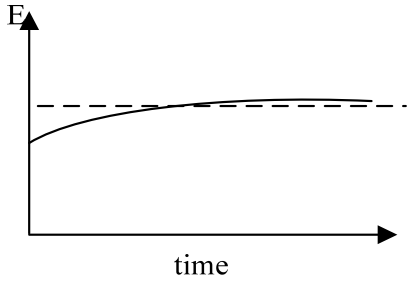

Figure 2. Development of Testing Environment Performance

The actual testing environment includes indoor field and outdoor field, but the outdoor field is often uncontrollable, so the indoor testing field is a preferential option as far as possible when the measure conditions allow. The indoor environment named anechoic chamber, it is a closed metal room that prevents the outside electromagnetic wave from penetrating into the interior, and the inside electromagnetic wave also can't escape to the outer space. Absorbing materials are installed on the wall as well to suppress internal reflection of electromagnetic waves. Due to the anechoic chamber shielding effect is stable, the comprehensive performance E of testing environment is approximately considered as a fixed value, and will not change obviously in a long time. Figure 2 shows the development of environment performance, solid line represents the actual performance development, dot line represents the trend.

As for the test instrument, the signal process ability is critical. The receiver should be capability of wide receiving bandwidth, high sensitivity and resolution, large dynamic range, real-time process, high-volume data coding and storing without any loss. The oscilloscope also should have wide bandwidth, high sample rate and large storage depth. And the spectrum analyzer's dynamic range, sensitivity, RBW and VBW is important. Figure 3 shows the oscilloscope bandwidth development in the last years, the time of bandwidth increased from 30GHz to 45GHz is 5 years, but from 45GHz to 60GHz just only 3 years[11].

The increase of test equipment comprehensive performances primarily depends on the development of electronic technology. Today Moore Law represents the development of electronic technology is still valid, so the attribute C of test equipment is positively correlated with the Moore law and the value C of test equipment performance is approximately a nonlinear increasing function of time just as the Figure 3 shows. Figure 4 shows the development of testing equipment performance, solid line represents the actual performance development, dot line represents the trend.

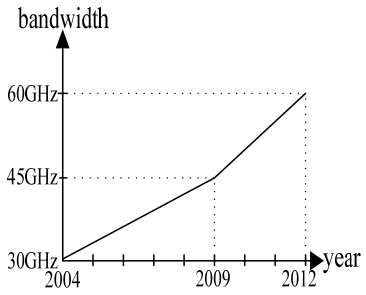

Figure 3. Development of Oscilloscope Bandwidth

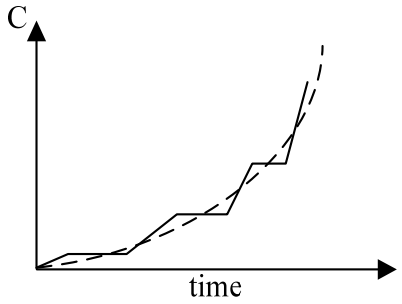

Figure 4. Development of Testing Equipment Performance

The attribution M of red signal analysis methods is decided by the level of the awareness of Red/Black signal. People first realize that the synchronal signal and pixel clock of display are red signals, they can be intercepted and then reconstructed [12].

In 1985, Van Eck successfully demonstrated that the screen content of a CRT display can be reconstructed at a distance [1].

In 1999 Paul Kocher proposed DPA (Differential Power Analysis) method, and the following research did successfully get the encryption key out of an encryption chip from its power curve. The result shows that some useful information namely red signals can be extracted from the power, and changed our understanding of the radiation signal of power.

So with the development of research, some electromagnetic radiation originally thought to be black signal is not real 'black', the radiation also does carry red signal. Figure 5 shows the Law curve of people's recognition of the red signal, solid line represents the actual development, and dot line represents the trend. With the deepening of research, the red signal identification method will be more mature, M can be seen as a linear growth trend approximately.

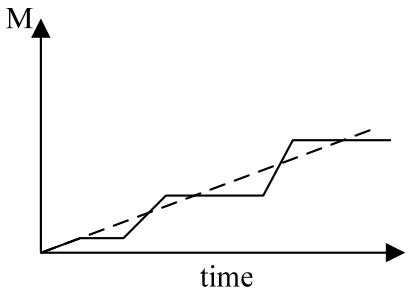

Figure 5. Development of Red Signal Analysis Method

In conclusion, all of the above four factors T, E, C and M which vary in different Law curve have come together to increase the accuracy of test result X. Among the four factors, three factors T, E and C are hardware related. E is approximately a constant, T is an approximately linear increasing value and C is an approximately nonlinear increasing value, obviously, C has the most impact on the result X.

4. Security Level Setting

After obtaining the testing result, how to judge the EUT security level needs to be considered seriously. It involves two sections needed to get balance: the establishment and maintain of test standard, the usage of security equipment.

Adopting the pass rule is suitable for the sake of reducing the work of standard establishment and maintain. But the actual security needs are not exactly the same, this pass rule will result in excessive safety protection or the opposite side-- insufficient safety protection. Adopting grading rule can avoid protection excessive or insufficient, but this rule increases the work of standard establishment and maintain.

How to grade that needs to be studied. In practical application, the current TEMPEST standard of USA and NATO adopts the grading rule [13]. Table 1 shows the detail.

Table 1. TEMPEST Grade Standard of USA and NATO

Standard Description	Security Level		
	Full	***Intermediate***	***Tactical***
NATO SDIP-27 standard	Level A	Level B	Level C
Previous NATO Laboratory Standards	AMSG-720B	AMSG-788A	AMSG-784
NATO Zoning Standards	ZONE 0	ZONE 1	ZONE 2
USA NSTISSAM /1-92 standard	LEVEL I	LEVEL II	LEVEL III

So the function of test result and grade level can be expressed as the following Equation (3).

$$S = \phi(X, B) = \left\{ \begin{array}{c} S_1 \middle| X \in [B_0, B_1) \\ S_2 \middle| X \in [B_1, B_2) \\ \vdots \\ S_n \middle| X \in [B_{n-1}, B_n) \end{array} \right\} \tag{3}$$

S represents the security level, X is the test result, B is an array of safety threshold for radiation field intensity $(B_0 < B_1 < B_2 < \cdots < B_n)$, ϕ is a piecewise function classified into $S_1, S_2, \cdots S_n$. The relationship is showed in Figure 6.

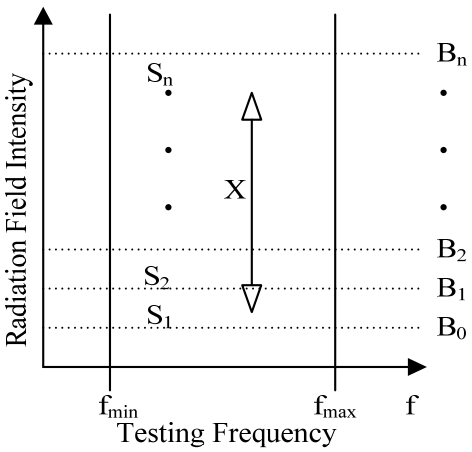

Figure 6. Security Level Grade

Need to explain that the test result X in Equation (1) which represents the information leakage emanate from EUT is hard to describe, because the practical quantity of information leakage depends on the attribution M.

The compromising electromagnetic emanations involve three stages: emanation, capture and reconstruction. To achieve the purpose of information security protection needs to prevent emanation firstly, so TEMPEST standard set the emission limits which require the radiation level must lower than the EMC standard. For example, the radiation level of information equipment which meet NACSIM5100 TEMPEST standard is 40dB-60dB much lower than the similar equipment which meet MIL-STD-461/462D EMC standard.

Therefore, the test result X uses radiation level to describe the compromising electromagnetic emanations.

The rationality of security threshold B can be rectified by the statistics of all information equipments' security level. And the grading rules should meet the actual security needs and archives the optimization of performance and cost. If the statistics of all equipments' security level in one period is normal distribution, then the setting of B is rational.

5. Conclusion

This paper proposes a mathematic model of TEMPEST test by analyzing the four key factors which influence the test result, and points out the development Law curve of the factors and the rationality check of security threshold B. These results will contribute to the further research of improving test accuracy and the analysis of trigger point to update TEMPEST test standard, and hope to promote the construction of TEMPEST standard.

References

[1] W van Eck. *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?* Computers & Security. 1985; 4: 269–286.
[2] Markus G Kuhn. *Security limits for compromising emanations*. Cryptographic Hardware and Embedded Systems, LNCS 3659, Springer. 2005: 265–279.
[3] Robert RG Yang, Thomas TY Wong. *Electromagnetic Fields and Waves.* Higher Education Press, 2006: 353-399.
[4] T Tominaga, M Masugi. *Overview of Electromagnetic Wave Security Guidelines.* ITU-T/SG5, TD143, 2005: 1-11.
[5] Jurong Hu, Xuning Zhu, Long Chen. *Electromagnetic Environment and Target Simulator for Radar Test.* TELKOMNIKA Indonesia Journal of electrical Engineering. 2013; 11(7): 3699-3703.
[6] Mao Jian, Li Yongmei, Liu Min. *Research for Data Erasure Based on EEPROM*. The 5th International Conference on Computer Science & Education. 2010: 1377-1379.
[7] Liu Jinming, Mao Jian, Li Yongmei. *Designing Eraser of Secret Information in EEPROM*. in 5th International Conference on Computer Science & Education. 2010.
[8] Zhang Jiemin, Li Yongmei. *The Study of The Standards Architecture and The Standards Attributes Based on EMC Standards and TEMPEST Standards in Computer System.* The 8th International Conference on Computer Science & Education, in Colombo, Sri Lanka. 2013.
[9] Karine Gandol, Christophe Mourtel, Francis Olivier. *Electromagnetic Analysis: Concrete Results*. Cryptographic Hardware and Embedded Systems. 2001; 2162 of Lecture Notes in Computer Science.
[10] Yuichi Hayashi. *Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current*. IEICE Transactons on Electronics. 2012; E95-C(6).
[11] H Tanaka. *Information leakage via electromagnetic emanationsand evaluation of tempest countermeasures*. Third International Conference on Information Systems Security, LNCS 4812, Springer. 2007: 167–179.
[12] Tang Minan, Wang Xiaoming, Yuan Shuang. Site Selection of Mechanical Parking System Based on GIS with AFRARBMI. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11(7): 3935-3944.
[13] US CNSS (the Committee on National Security Systems). *Index of National Security Systems Issuances*. 2012