

Study on TEMPEST Standards Attributes and Architecture

Zhang Jiemin

Computer Engineering College, Jimei University, China
zhangjm169@163.com

Abstract

The paper study on the TEMPEST standards with not only analyzing a large number of data from decrypted and semi-decrypted documents, but also tie up with the EMC standards because of they are indivisible. It proposed three attributers on TEMPEST standard, including serializability, architecture and life cycle. The serializable standard means no conflicts, including but not limited to, of the standards specifications, issue times, data limits, publishers, practitioners and so on. The architecture of standard exists so that should be named in nomenclature and demonstrated with systematic way. The standard should be established and published on opportune moment, living cycle from established to cancelled. The attributers are demonstrated through TEMPEST standard examples. The development of TEMPEST standards should be consistent with TEMPEST theories and products.

Keywords: Data Security, TEMPEST, Information Equipment, Compromising Emanations, Standards Architecture

1. Introduction

All electrical and electronic equipment produces electromagnetic radiation. The electromagnetic signals propagate along electrically conductive pathways called conducted emissions or through space called radiated emissions. The conducted emissions and the radiated emissions both will result in electromagnetic interference (EMI) and electromagnetic leakiness [1-3].

EMI is a process by which disruptive electromagnetic energy is transmitted from one electronic device to another via radiated or conducted paths or both [2, 3]. In common usage, the term refers particularly to Radio Frequency signals, but EMI can occur in the frequency range from direct current to daylight.

Electromagnetic leakiness is more severe rather than merely EMI. If these emissions are intercepted and analyzed they could reveal that the signals contain information and thus the protectively marked data could be revealed. A receiving device can intercept these signals without being detected even when located some distance away access to the original equipment is not required.

Electromagnetic testing examines the power of the emissions to ensure the tested item will not adversely affect other products in the locality and will not it be adversely affected. Emission levels are set by rules and regulations as mandate from national and international organizations. The standards on emission levels be classified into two types, one is EMC (Electromagnetic Compatibility) standards about EMI and the other is TEMPEST standards about electromagnetic leakiness.

EMC is the ability of a product to coexist in its intended electromagnetic environment without causing or suffering functional degradation or damage. The system has to achieve acceptable levels of electromagnetic compatibility.

TEMPEST is originally a codeword since declassified rather than an acronym [3, 4]. Nowadays TEMPEST is defined as the study of the unintentional emission of protectively marked data from an equipment or system. It's the subject derived and distinguished from

the theory of EMC. Even the existence of the study and countermeasures was highly classified. All details of testing, signals, limits, test results and countermeasures remain protectively marked to a very high level. The study on the TEMPEST standards must analyzing a large number of data from a huge mass of decrypted or semi-decrypted documents refer to the EMC standards or the TEMPEST standards , having accumulated for a long time.

2. Definition of the Standards

The definition of standards as the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) in 1996 is “Document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, aimed at the achievement of the optimum degree of order in a given context.”, The documents on standards are stated that “guideline documentation that reflects agreements on products, practices, or operations by nationally or internationally recognized industrial, professional, trade associations or governmental bodies”.

In 2002, the national document of China "GB/T 20000.1-2002 states the definition of standards in "standardization and related activities of the general vocabulary": in order to within a certain range for the best order, develop and by consensus by the recognized authority for approval, common use and repeated use of a normative document. Note: standard should be based on science, technology and experience based on achievements, to promote the best common benefits for the purpose of”.

Thus the definition of standards as ISO/IEC is accepted in China. In fact, the major organizations for standardization in the international follow the ISO/IEC. It was released in 2004 the latest version on the definition of standards as ISO, but not was changed than in 1996.

3. About Recognized Body

A recognized body is an organization such as ISO consisted of the members that can voluntarily reach a consensus focus on some issues in a area. Objectively, it's present that non-compliance on a recognized body stated in the definition of standard in China. In China, the national standards are established and issued by the Standardization Administration of the People's Republic of China (SAC). The trade standards or the industry standards are established and issued by the central regulatory agency. The regional standards are established and issued by the local bureau of quality and technical supervision. The standards published by these organizations above have the common feature of government permission in China. In one respect, the feature is good for the standards popularization. The government bodies are stronger about enforcing the standards than the recognized bodies. In another respect, the agreements of members must be reflects fully in government bodies for the reasonable standards established.

4. Opportunity for Establishing Standards

The establishing of standards must be took the opportunity. It's inappropriate not only earlier but also more latter, showed as Figure 1.

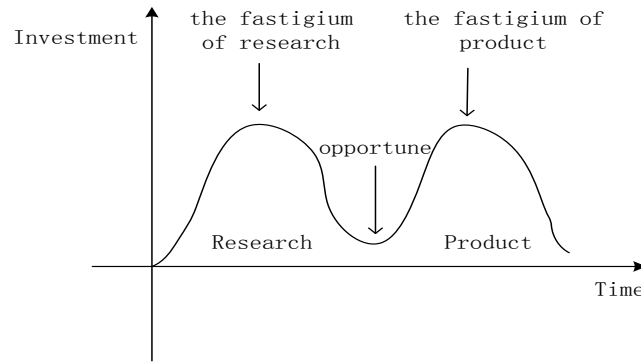


Figure 1. The Opportunity for Establishing Standards

The trough is an opportunity for establishing and issuing standards so that the standards embodying research findings can guide the productive process effectively. In the earlier until the fastigium of research, the theory matures not enough to establishing the standards. Later the fastigium of product, to the contrary, the being investing heavily leads to results to obey the standards so difficultly.

The real standards may be established while the regulation standards be later the opportune moment. It is the one of example typically that TCP/IP in contrast OSI/ISO. The real standards on EMC, after adoption and publication by the European Parliament, are prefixed with "EN", as showed in Table 1. In fact, as members of the EN (European Normalizations) standards [2, 3], it is common to be refer to international specifications as IEC.

Table 1. The Real Standards on EMC as IEC in 1993-1994

The Number of Standard Documents	The Name of Standard Documents
EN 50 082-1: 1993	Electromagnetic compatibility generic immunity standard—Part 1: Residential, commercial and light industry
EN 55 013: 1993	Limits and methods of measurements of radio disturbance characteristics of broadcast receivers and associated equipment
EN 55 014: 1993	Limits and methods of measurements of radio disturbance characteristics of household electrical appliances, portable tools and similar electrical apparatus
EN 55 020: 1993	Limits and methods of measurements of radio disturbance characteristics of broadcast receivers and associated equipment
EN 50 081-2: 1994	Electromagnetic compatibility generic emission standard—Part 2: Heavy industrial environment
EN 50 082-2: 1994	Electromagnetic compatibility generic immunity standard—Part 2: Heavy industrial environment

Analyzing the Table 1 showed that it is necessary to set down these additional real standards as remedy for the regulation standards. The standards prefixed with an “EN 50 081” should be on electromagnetic compatibility generic emission. The part one of “EN 50 081” refers to the residential, commercial and light industry complies with the standard published in 1992. The part two of “EN 50 081” be adopted and published in 1994 refers to the heavy industrial environment. The standards prefixed with an “EN 50 082” should be on electromagnetic compatibility generic immunity. The part one of “EN 50 082” be adopted and published in 1993 refers to the residential, commercial and light industry. The

part two of “EN 50 082” be adopted and published in 1994 refers to the heavy industrial environment. It'll take some time to convert the real standards into the regulation standards.

5. Development of the Standards

The beginning time is so different for various country focusing on TEMPEST that each country has its own condition. The sooner the country starts, the more the published versions of standards. The United States pay close attention to the TEMPEST on the earliest time, they had made greater progress than others, showed in Table 2.

Table 2. The Updated TEMPEST Standards (up to 2012)

Publisher	The Earliest Release Time	Updated
the United States	in 50s of the 20th century	6 times
the North Atlantic Treaty Organization	in 1982	2 times
China	in 1994	1 times

The TEMPEST standards of the NATO updated from 2002 to 2005, showed in Table 3.

Table 3. Index of NATO TEMPEST Standards Issuances

Time	Title	Version	Note
in 80s of the 20th century	AMSG 720B AMSG 788A AMSG 784 AMSG 799B AMSG 719	Version 1	
in Nov 2005	SDIP-27	Version 2	Supersedes all previous editions : AMSG 720B AMSG 788A AMSG 784
in Nov 2005	SDIP-28		Supersedes the previous editions : AMSG 799B
in Jan 2006	SDIP-29		Supersedes the previous editions: AMSG 719
in 2002	SDIP-30		
No in details	SDIP-55		

The TEMPEST technology has been gradually developed and advanced continuously in USA and The TEMPEST standards has been revised the most times in all over the world. The newer nomenclature may attest the substance has be changed. such as the nomenclature of the standards changed from the abbreviation "NACS" to "NSTISS". The abbreviation "NACS" refers to "the National Communication Security", and the abbreviation "NSTISS" refers to "the National Security Telecommunications and Information Systems Security". The TEMPEST standards extend from the field of the communications security to the security of information system. The development of the TEMPEST standards is showed in Table 4.

Table 4. The Development of the TEMPEST Standards in USA

Issue Time	Standards	Note
in 50s of the 20th century	NAG-1A	
in 60s of the 20th century	FS222/ FS222A	Supersedes NAG-1A
in 70s of the 20th century	NACSEM 5100	Supersedes FS222
	NACSEM 5101	NACSEM 5100 series standard
	NACSEM 5106	
	NACSEM 5110	
	NACSEM 5204	
in 80s of the 20th century	NACSIM 5100A	Supersedes NACSEM 5100
	NACSIM 5203	
in 90s of the 20th century	NSTISSAM TEMPEST/1-91	Supersedes NACSIM 5100A
	NSTISSAM TEMPEST/1-92	Supersedes NSTISSAM TEMPEST/1-91
	NSTISSAM TEMPEST/2-91	Supersedes NACSEM 5106
	NSTISSAM TEMPEST/1-93	Supersedes NACSEM 5110
	NSTISSAM TEMPEST/2-93	Supersedes NACSEM 5101
	NSTISSAM TEMPEST/1-95	Supersedes NACSEM 5204
	NSTISSAM TEMPEST/2-95	Supersedes NACSIM 5203
	EMPEST 2-92	Supersedes all previous NACSEM 5100 series editions
in the 21th century	TEMPEST 1-00	
	TEMPEST01-02	

6. Standard Attributes and Architecture

The discussion on the attributes of standards may promote the development of standards. First, the standards running at the same time should be serializability. The serializable standard means no conflicts on the specification of standards each other, no conflicts on the time the standards issued, no conflicts on the limits of data, no conflicts in the publishers each other, no conflicts in the practitioners each other, even though no conflicts between the publishers and practitioners. Any conflict may lead to one invalid standard or more.

Second, the architecture of standards running exists. The relevant departments are now formulating a series of standards in accordance with the provisions of rules and regulations as mandate from national and international organizations. Internationally, each country has a designated agency within its government to oversee all aspects of communication in particular of TEMPEST. The architectures of TEMPEST standards of China are showed as Figure 2.

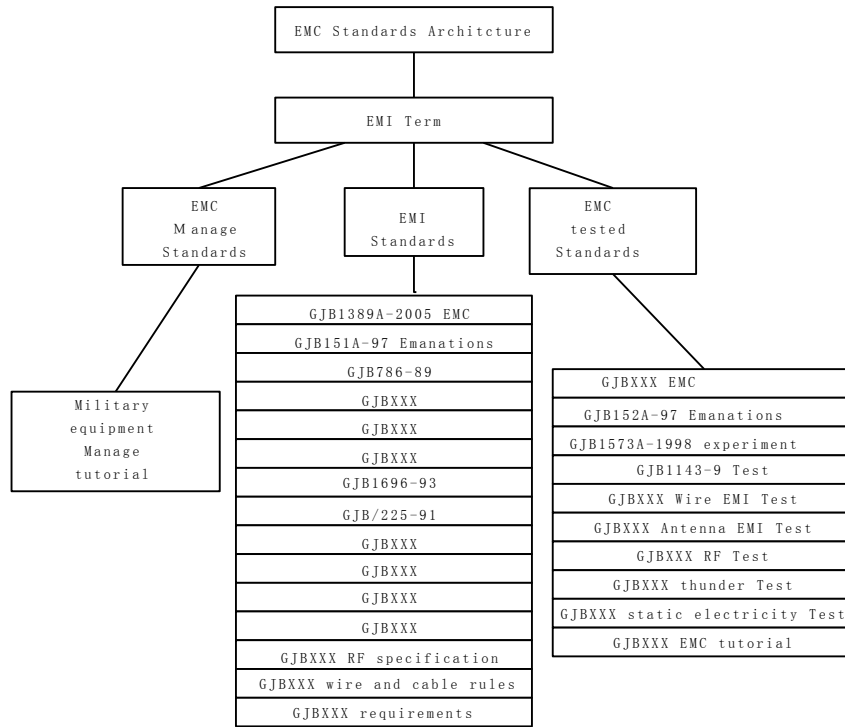


Figure 2. The Architectures of TEMPEST Standards of China

The variations of the organizations of America on the TEMPEST standards in nomenclature and in substance are showed in the Table 5. That reveals the standard architecture from nomenclature.

Table 5. The Variations of Organizations of America in Nomenclature and in Substance

Abbreviation (Stand for the Series of Standards)	Full Name	Period
FCC	The Federal Communications Commission	1970's
NACSEM	National Communication Security Emanations Memoranda	1970's
NACSIM	National Communication Security Information Memoranda	1980's
NCSC	The National Center for State Courts	1980's
NSTISSP	The National Security Telecommunications and Information Systems Security Policy	1990's
NSTISSD	The National Security Telecommunications and Information Systems Security Directive	1990's

NSTISSC	The National Security Telecommunications and Information Systems Security Committee	1990's
NSTISSC	The National Security Telecommunications and Information Systems Security Instruction	1990's
CNSS	the Center for National Security Studies	2000's

The TEMPEST standards can be applied to testing the product safety. The products passed TEMPEST certification can be listed in recommended products. The higher the security level, the higher the cost. The computer including any devices can be tested with various degrees of rigor.

The United States or NATO is very seriously for the TEMPEST device partition and the special standards issued. The running standards divided the computer into three levels, showed in Table 6. That reveals the standard architecture from substance.

Table 6. The TEMPEST Standard on the Device Partition of USA & NATO

Publisher	Standards	Advanced	Intermediate	Primary
NATO	SDIP-27 Standard	Level A	Level B	Level C
NATO	Laboratory Standards (Previous)	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

The third attribute of standards is life cycle besides listed above. It's established from the national law refer to the regulation requirements adopted by the committees or organizations of the standards. It's cancelled or superseded while no guideline to the products. The faster the development of technology is, the shorter the life cycle of standards is.

The TEMPEST standards consist of some parts [6, 7]. It demonstrates the development history of TEMPEST standards consistent with the development of TEMPEST theories and TEMPEST products, as showed as Table 6.

Table 7. Updated on the TEMPEST Standards Consist of Parts

No.	Parts	April 2005/July 2012
1	Current Policies	17 / 19
2	Current Directives	7 / 8
3	Current National Communication Security Instructions	5 /
4	Current Instructions	59 / 77
5	Current Advisory Memoranda	31 / 33
6	National Communication Security Information Memoranda and Emanations Memoranda	3 / 3
7	Annex A Cancelled or Superseded issuances	115 / 140
8	Other CNSS Issuances	/ 8

7. Standardization in China

Compared with the other country in the world, such as USA, we still have a long way to go. The current TEMPEST standards in USA are showed in Table 8.

Table 8. The Current TEMPEST Standards in USA (up to 2012)

Code Name	Nomenclature	Title	Issue Time
7000	CNSS	TEMPEST Countermeasures for Facilities (U)	May 2004
7001	NSTISS	NONSTOP Countermeasures (U)	Jun 1994
7002	NSTISS	TEMPEST Glossary (U)	Mar 1995
TEMPEST 2-91	NSTISS	Compromising Emanations Analysis Handbook (U)	Dec 1991
TEMPEST 1-92	NSTISS	Compromising Emanations Laboratory Test Requirements, Electromagnetics (U)	Dec 1992
TEMPEST 2-92	NSTISS	Procedures for TEMPEST Zoning (FOUO)	Dec 1992
TEMPEST 1-93	NSTISS	Compromising Emanations Field Test Requirements, Electromagnetics (U)	Aug 1993
TEMPEST 2-93	NSTISS	Rationale for Compromising Emanations Laboratory and Field Test Requirements, Electromagnetics (U)	Oct 1993
TEMPEST 1-95	NSTISS	Shielded Enclosures (U)	Jan 1995
TEMPEST 2-95	NSTISS	RED/BLACK Installation Guidelines (U)	Dec 1995
TEMPEST 1-00		Maintenance and Disposition of TEMPEST Equipment	Dec 2000
TEMPEST01-02	CNSS	Non-stop Evaluation Standard	Oct 2002

The current TEMPEST standards in China are showed in Table 9.

Table 9. The Current TEMPEST Standards in China (up to 2012)

Nomenclature-Code Name	Title
BMB1-1994	Telephone Compromising Emanations limits and test Requirements, Electromagnetics
BMB2-1998	Compromising Emanations equipments Test Requirements and safety criterion, Electromagnetics
BMB3-1999	Compromising Emanations shielding devices for secret information equipments technical specifications and Test Requirements
BMB4-2000	EMI units technical specifications and Test Requirements
BMB5-2000	Compromising Emanations Field for secret information equipments Limits and Test Requirements ;
BMB6-2001	Crypto equipments Compromising Emanations Limits
BMB7-2001	Rationale for Crypto equipment Compromising Emanations Test Requirements

BMB7.1-2001	Crypto Telephone Compromising Emanations Test Requirements
BMB8-2004	TEMPEST product Laboratory Test Requirements,
BMB19-2006	Shielding cabinet technical specifications and Compromising Emanations Test Requirements
GGBB1-1999	information equipments Compromising Emanations limits
GGBB2-1999	information equipments Compromising Emanations Test Requirements
BMB9.1-2007	mobile communication interference units in Confidential meeting room Test Requirements
BMB9.2-2007	mobile communication interference units in Confidential meeting room Installation Guidelines

Analysing the Table 8 and the Table 9 and studying the materials associated with TEMPEST standards. The difference of TEMPEST standard between China and USA is showed in Table 10.

Table 10. The Difference of TEMPEST Standard Between China and USA

TEMPEST Standards	USA	China
TEMPEST Standards	Exists	No released
TEMPEST Countermeasures for Facilities	Exists	No released
TEMPEST Glossary	Exists	No released
Compromising Emanations Analysis Handbook	Exists	Exists
Compromising Emanations Laboratory Test Requirements	Exists	Exists
Rationale for Compromising Emanations Laboratory and Field Test Requirements	Exists	No released
Procedures for TEMPEST Zoning	Exists	No released
Shielded Enclosures	Exists	Instructions only on the Interference Units
RED/BLACK Installation Guidelines	Exists	No released
Maintenance and Disposition of TEMPEST Equipment	Exists	No released

8. Conclusion

The standards should be established and published on opportune moment. It may lead to the unsuccessful standards issued too later or too earlier. In this paper, the attributes of standards are defined as serializability, standard architectures, life-cycle and so on. The serializable standard is directed to avoid conflict of, including but not limited to the standards specifications, issue times, data limits, publishers and practitioners each other, even though no conflicts between the publishers and practitioners. The architectures of standard appear to with being systematic demonstrated. A suit of standards be named in nomenclature. It is the fact of existence that non-compliance on a recognized body with stated in the definition of standard in China, but the feature is good for the standards popularization on the other hand. Now the TEMPEST standards extend from the field of the communications security to the security of information system and China has a long way to go. To study on standards will pushing forward the standardization process. The TEMPEST standardizations is of great importance to information security.

References

- [1] E. Benedict, "PCB Design for EMI/EMC Compliance", WEMPEC Seminar, **(2000)**.
- [2] M. I. Montrose, "Printed Circuit Board Design Techniques for EMC Compliance", Published under the Sponsorship of the IEEE, **(1996)**.
- [3] Sponsored by the Accredited Standards Committee C63, American National Standard Dictionary of Electromagnetic Compatibility (EMC) including Electromagnetic Environmental Effects (E3), **(2009)**.
- [4] Electromagnetic Compatibility Society, **(2002)**.
- [5] SST TEMPEST Introduction iss 3, TEMPEST Introduction, **(2010)**.
- [6] "U.S. Government contractors should contact their Contracting Officer Representative regarding distribution of these documents", Index of National Security System Issuances, **(2012)**.
- [7] "U.S. Government contractors should contact their Contracting Officer Representative regarding distribution of these documents", Index of National Security System Issuances, **(2005)**.