Investigation of the Risk of Electromagnetic Security on Computer Systems

Changlin Zhou, Member, IACSIT, IEEE, Qun Yu, and Litao Wang

Abstract—Electromagnetic environmental effects (E3) and compromising emanations (CE) are two centrally important aspects of computer closely related to electromagnetic security. This paper investigates the electromagnetic compatibility (EMC) for functional safety and emission security on computer systems. Initially, the EMC security issues for the electromagnetic emission of computer systems as well as the susceptibility of tremendously increased critical circuits are presented. Then, impact of electromagnetic security in ubiquitous applications based on computer technology is discussed, which encompasses the damage of E3 and risk potential. CE security limits and experiment example of TEMPEST. Finally, the protection means of computer electromagnetic security are provided. The paper states the need for the guidelines on controlling EMC and the process of CE to achieve electromagnetic security of computer systems.

Index Terms—Electromagnetic compatibility (EMC), electromagnetic environmental effects (E3), compromising emanations (CE), functional safety, emission security, computer

I. INTRODUCTION

One of the important problems peculiar to computer systems is electromagnetic emission and immunity, as known as EMC for electromagnetic security [1], [2]. All electronic technologies rely on computer systems which are being applied in very sensitive installations, and can suffer from degraded functionality, malfunctions and even permanent damage due to electromagnetic interference (EMI) [3], [4]. The computer systems may be commercial or industrial performance dependent on the correct operation, and may be military or government sensitivity where functional safety or even information security is at risk [5], [6].

As computer systems is increasingly used in safety-related applications, the real world risks of electromagnetic security are involved twofold [7]. There are the relatively functional safety damage of disruption of computer systems from external influences [8]. And, there are the emission security risks of sensitive information leaking out of the computer systems [9]. Consequently, with an increasing risk of electromagnetic security for computer systems architecture due to inadequate EMC can result in hazardous situations [10], [11]. Important issues of EMC-related functional safety and compromising emanations (CE) may be correctly addressed [12]-[14].

This paper is to raise the awareness of electromagnetic security issues for computer systems and networks. It describes to achieve due diligence for functional safety, and introduces the comprehensive risk defending methodology to control CE for information security.

II. ELECTROMAGNETIC SECURITY OF COMPUTER

EMC is the scientific and engineering discipline of ensuring that electrical or electronic technologies not emitting high levels of EM energies that cause excessive EMI [1]. It is also concerned with ensuring that they do not suffer untoward EMI during operation. Achieving electromagnetic security and safety of computer systems means that risks due to EMC will remain no worse than tolerable over the anticipated lifetime.

A. EMC Issues of Computer Systems

The EMC of computer systems is the ability of system or networks to function satisfactorily in its Electromagnetic environment (EME) without introducing intolerable EMI to anything in that environment. Modern computers and other types of information equipment using microprocessors and IC devices appear to be vulnerable and sensitive to EMI. Following the scale down of the IC technology, the operating frequency has increased and the supply voltage has become lower, the EMC problems at computer systems level have recently risen in importance. The two major keywords in EMC issues are shown as Fig.1, and the characteristics of emissions and susceptibility must remain at least adequate.

Computer systems susceptibility to EMI is becoming a major concern, with the multiplication of powerful electromagnetic sources such as mobile phones, high speed networks, wireless systems and intentional EMI (IEMI). High frequency wave and power pulse are received by the systems, which captures some energy that may flow to the interior, the board and finally to the component. As the supply voltages become lower, these devices manage various signals such as digital signal, communication protocol, external memory bus or external interrupt signal, which are potential paths to introduce EMI into inside circuits.

The emission due to computer clock and system frequency is continuously increased, and may jeopardize the correct...
behavior of other devices. The parasitic emission energy may be high enough to jeopardize the EMC of the whole electronic system. Finally, they cause damages on interior chips or some malfunction to systems. On the other hand, there are emission security risks of computer system for processing information. The EMC performance of computers could have implications for functional safety or security when these devices are used in communications systems and information equipments, safety-critical architecture or critical infrastructure.

B. EMC for Security of Computer Systems

The challenge of achieving EMC in the design of computer systems, particularly in the functional safety requirements and information processing security, has increased the needs for understanding, evaluating and improving the electromagnetic security performance of computer systems. Robust operation of complex systems and networks is essential for the computer deployed increasingly to monitor vital control and safety functions. Similar reliability standards are necessary in many other security appliances, ranging from nationality security to communications and even some consumer appliances.

Safety functions are increasingly performed by integrated electronic systems, such as computer systems architecture and networks. These computer systems are designed in such a way as to prevent dangerous failures from occurring or to control such dangerous failures to a tolerable level of occurrence. Such dangerous failures may be the consequence of random or systematic hardware failures, software errors, human errors or environmental influences including electromagnetic disturbances and IEMI. With respect to EMC, the correct and safe operation of a computer system depends on the electromagnetic environment of intended use, the immunity level of the integrated system, mitigation measures applied, and the performance criteria applied.

Emissions security includes conductive coupling such as power and network wires, and radiated coupling acts as an equivalent antenna and transmits undesired electromagnetic waves. Typical compromising emanation security problems appear due to undesired coupling of data wire and ribbon cables in direct and indirect emanations from computer display, and keyboards and network, when data is encoded with logic states transition and electromagnetic waves are eventually emitted. Electromagnetic emanations may interact with indirect emanations which induce new types of radiations. And these unintended emanations manifest themselves as modulations or inter-modulations or as carrier signals and their harmonics, and may have better propagation than direct emanations for information security.

III. IMPACT OF ELECTROMAGNETIC SECURITY

A. EMI Impact Analysis on Computer Systems

EMI impact is about the hazard and risk associated with electrical and electromagnetic environments. The impact of electromagnetic is perhaps the best captured in the immunity limits to computer systems. The EMI coupling can occur either via antennas and sensors, denoted front-door coupling, or as back-door coupling, i.e. through imperfect shields or to cables. A basic decomposition of an EMI impact can be described as the schematic sketch as Fig.2. There are more than scientific curiosities to fuel the research of EMC.

The source (1.) is creating an electromagnetic field or a voltage and current transient which propagate along the coupling path (2.). The source can be categorized according to many characteristics, and mode of emission must be considered. The coupling path (2.) includes conduction as voltage and current propagating along a conductor, and radiation as electric and magnetic energy emitting into the space. The system exterior (3.) will highly influence the coupling of the energy to the system interior (4.) and finally interact with the response or impact of potential critical component in the system (5.).

To reduce the impact of the affected system, the EMC is done by minimizing the transfer function between the source and the receiver. So to the typical computer systems, the disturbances source is expressed in the function of $S(t,f,r,\theta)$, which is figured by time variable $t$, frequency variable $f$, space variable $r$ and orientation variable $\theta$. Also the coupling way and target interfered response elements are expressed by $C(t,f,r,\theta)$ and $R(t,f,r,\theta)$. Then the EMC performance of the system can be assessed with inequation (1) when electromagnetic interference happens.

$$S(t,f,r,\theta)\bullet C(t,f,r,\theta) > R(t,f,r,\theta)$$

(1)

where, the interference safety margin $M$ can be given as an equation (2).

$$M = R(t,f,r,\theta) - S(t,f,r,\theta)\bullet C(t,f,r,\theta)$$

(2)

Obviously, $M > 0$ indicates a potential interference, $M < 0$ that is compatible with both work, $M=0$ that is in critical condition. Interference of the corresponding parameter is the EMC prediction equation based on the actual mathematical model for computer systems, combined with analysis of the equation and the corresponding solutions. Normally, -6 to -10 dB for $M$ is taken to be the safety factor, so resistance based on the actual evaluation results.

It is expected to competently ensure a minimum margin $M$ of the desired levels of safety risks. For higher safety integrity levels it may be necessary to have a higher compatibility level of confidence. Thus the susceptibility or immunity levels specified in EMC standard series may be sufficient for safety-related functions implemented. The computer system functional safety perspective on EMC must be addressed, and provide guidance for evaluating and designing to the appropriate requirements.
B. Risk Potential of Electromagnetic Effect

The risk of E3 upon the operational capability of computer systems, and electromagnetic pulse (EMP), high power electromagnetic (HPEM) or IEMI sources is mostly considered in the victim system [2]. Computer is sensitive to exposure to EMP, as any cables running in and out of the equipment will behave very much like antennae, in effect guiding the high voltage transients into the system interior. Computers used in communications systems, and industrial control applications, and embedded in military equipment are all potentially vulnerable [5], [15].

There are several threat phenomena and effects that can take place and cause serious problems of interference or damage for computer systems. The different upset events can be classified according to risk assessment of IEMI or HPEM environments disturbance scale [16]. An alternate method, based on the variables threat level, consequence, and susceptibility of the computer systems and networks is suggested [17]. These three variables form a vulnerability vector in the variable space spanned which is shown as Fig. 3. The scaling of these variables can be collectively be weighted and estimated by forming a numbered scale and grading. In a final assessment stage the values of all three quantities are concluded into the general risk potentials of the considered electromagnetic environment.

- **Threat level.** The parameter threat level, where a high threat level characterizes a high risk, describes the ability of the HPEM environment to cause IEMI effects. The threat level is perhaps the aspect of an HPEM environment which has been mostly investigated and evaluated by the EMC community. In related publications attributes of the radiated field, i.e. amplitude (Epeak), far radiated voltage (r-Epeak) and waveform characteristics, and the frequency range is from 100MHz to 10GHz. The threat level on computer systems can be represented by a threat vector as Table I. The scaling of these variables can be collectively be weighted and estimated by forming a numbered scale and grading. In a final assessment stage the values of all three quantities are concluded into the general risk potentials of the considered electromagnetic environment.

- **Consequence.** The consequence term is to investigate the number of existing connections in relation to the attacked computer systems, and a successful attack on a well connected system is often higher than one that is not connected. The criticality of these connections is of importance as a centralized system and larger grid infrastructure would collapse a great number of other systems would be directly affected. Loss of connections between systems could be a consequence of a successful IEMI attack. The consequence could be measured as lost connections and represented by a numbered scale and complication vector as Table II.

| TABLE I: THREAT LEVEL VARIABLES CLASSES CHARACTERIZATION |
| --- | --- | --- |
| Category | Effect | Description | Value |
| 0 | No effects | Functional safety | ≤10V/m, ≤1kV |
| 1 | Cause disturbances | Interference, Wrong data | 100V/m, 10kV |
| 2 | Strong interference | Crash, State change | >1kV/m, 100kV |
| 3 | Mission kills | Loss of function and data | 10kV/m, 1MV |
| 4 | Physical damage | Destruction, Repair or replace | 100kV/m, 10MV |

- **Susceptibility.** The susceptibility term expressed the computer systems to perform without degradation in the presence of an electromagnetic disturbance. Standard EMC susceptibility tests are made by subjecting the objects under test for disturbances and field levels for different situation and their corresponding upset events. Susceptibility terms can be estimated from susceptibility tests performed on subsystems or equipment either considered critical for the operation of the facility or easily accessible by an electromagnetic disturbance and standard EMC requirements as Table III.

| TABLE II: CONSEQUENCE VARIABLES CLASS CHARACTERIZATION |
| --- | --- |
| Category | Description | Lost Value |
| 0 | No connections any cable, battery supply | ≤10% |
| 1 | Stationary computer host, mains power feed and data wiring | 10% |
| 2 | Computer systems architecture, platform and connections local area network | >25% |
| 3 | Computer network, large associate platform and communication network | 50% |
| 4 | Complex architecture, infrastructure and global information grid | >80% |

| TABLE III: SUSCEPTIBILITY VARIABLES CLASS CHARACTERIZATION |
| --- | --- |
| Category | Description | Value |
| 0 | Highly sophisticated system, robust hardening strategies | Margin of at least 16.5 dB of MNFS |
| 1 | No susceptibility | Margin of at least 6 dB of MNFS |
| 2 | No sensitivity | MIL-STD-461F requirements |
| 3 | Sensitivity, common equipment not hardened against HPEM | Commercial EMC standard tests |
| 4 | Less than the level of immunity for common equipment | No commercial EMC tests |

IV. IMPACT OF EMANATIONS SECURITY

Information leakage via electromagnetic emanation or emanations security (EMSEC) from computer systems is a well known security risk. An eavesdropper receiving electromagnetic emanations does not leave evidence of their activity, and the victim notices nothing, various countermeasures have been proposed for such “TEMPEST” problems.
A. Emission Security Limits for Computer Systems

Emission limits and test procedures require its actual conformance standards for electromagnetic security of computer systems. Current means for such efforts could be the work that leads to the emission limits for EMC, to reduce the risk of information carrying emanations. The emissions limits therefore have to be based on an understanding of reasonable best-case assumptions of the minimal background noises that the eavesdropper faces even under good receiving conditions. One approach to designing an emission security standard is to provide an upper bound for the signal-to-noise ratio \( S/N \) that an eavesdropper could achieve. The major contributing factors be considered are shown in equation (3).

\[
S / N = \frac{E_B \cdot G_a \cdot G_p}{a_d \cdot a_w \cdot E_{\text{eb}} \cdot f_r} \tag{3}
\]

where \( E_B \) is the maximum field strength that the test standard permits, \( B \) is the impulse bandwidth used in the test, \( ad \) is the free-space path loss, \( aw \) is the additional attenuation caused by building walls, \( Ga \) is the gain of the best directional antenna, \( Gp \) is the processing gain, \( E_{\text{eb}} \) is the field strength of natural and man-made radio noises at the location of the eavesdropping antenna within a bandwidth \( B \), \( f_r \) is the noise factor of the eavesdropper receiver.

Suggested emission limits require \( S/N < 0 \text{ dB} \) and use all of the just listed parameters in equation (3), and a result can be ended up with \( E_B \) and \( E_{\text{eb}} \) strength. It would be desirable if the suggested limits are verifiable with EMC measurement equipment. The EMC standard such as MIL-STD-461F provides in its requirement RE102 for mobile computer systems radiated electric limits field to those suggested here. The limits discussed here are aimed at products in which emission security is achieved by signal suppression and shielding and attenuation to be achieved protection standards.

B. The Recovered Result from Electromagnetic Emission

Computer systems can emit electromagnetic signals from which eavesdroppers may reconstruct processed data at some distance, known as TEMPEST issues on investigations of CE referring to national security information [10]. TEMPEST is often used broadly for the entire field of emission security for information systems from potential eavesdroppers and the ability to intercept and interpret those signals from other sources. In typical computer communication or data processing systems, undesired signal emanations will probably be detected when the equipment must be proven TEMPEST hazard-free. The most easily recognized CE is the RED (sensitive information) signal. This type of CE is generated as a carrier being usually amplitude or angle-modulated by the RED data signal.

The mostly impulsive emanations of TEMPEST signals can be radiated into space or coupled into external conductors. The modulated spurious carrier and impulsive emanations with the operating computer can be seen on a line or through the air. Here is an example of TEMPEST information from computer systems, shown as Fig. 4. The (a) is PC screen display word message, and the (b) is eavesdropper from a monitor at 10m distance. This result shows that we can monitor emanated electromagnetic signal corresponding to the screen image, and that the countermeasures are important and necessary.

V. PREVENTION OF ELECTROMAGNETIC SECURITY

The risk avoidance of a lack of proper function due to IEMI or HPEM and the lack of confidentiality due to EMSEC can be advanced level of the EM mitigation of the computer systems. An integral design guideline is needed to achieve an optimum cost-effective integration of technologies at the level of chip, board, cable, network, and system architecture.

A. EMC Design Guidelines for Functional Safety

Traditional approaches to improving immunity include adding filtering and shielding to protect the electronic systems against IEMI. Specific design techniques or embedded software approaches may also be used. Focusing on the microcontroller world, part of the hardware problems due to EM susceptibility may be handled by using software solutions aiming at reinforcing the robustness of the embedded systems. The effectiveness of defensive software to protect computer systems against IEMI or HPEM disturbances is strongly dependent on the application and the threat level. And, in the case of more powerful disturbance, hardware-based recovery mechanisms and redundant storage of the most crucial system might help handle this type of interference.

Four important EMC design guidelines to functional safety are often adopted to implement early in the computer design process. Firstly, minimize the loop areas associated with high frequency power and signal currents. The path of least impedance at high frequencies is generally the path of least inductance, and currents return as close as possible to the path of the outgoing current, which are generally the path that minimizes the loop area. Secondly, don’t split, gap or cut the signal return plane. The thumb rule is to provide one solid plane for returning all signal currents. Thirdly, don’t locate high speed circuitry between connectors as relatively efficient antennas can easily develop potential differences of mill volts. These voltages can drive currents onto attached cables causing a product to exceed radiated emissions requirements. Fourthly, control signal transition times which can cause signal integrity and thermal problems. The common methods use a logic family as fast as the application requires, put a resistor or a ferrite in series and a capacitor in parallel with a devices output.

Some good design guidelines of circuit board layout generally offer good advice. A device on the board that communicates with a device off the board through a
connector should be located as close as possible to that connector. All off-board communication from a single device should be routed through the same connector. Active digital components should be selected that have maximum acceptable off-chip transition times. Critical signal traces should be buried between power or ground planes. A trace with a propagation delaying more than half the transition time of the signal it carries must have a matched termination. Signals with high-frequency content should not be routed beneath components used for board input and output (I/O). The length and the number of vias in high-frequency nets should be minimized. Connections should be made by using via adjacent to the power or ground pad of the component.

Total computer systems architecture level guidelines for EM safety threats are based on two factors, which are general shielding of systems and filtering of I/O wiring. Metal shielding or thick concrete walls can achieve system protection. Protecting inputs and outputs is the main issue, and wires act as antennas special should be considered. The protections against IEMI and E3 are based on a breakthrough filtering technology. This filtering specifically protects the electronics against intentional aggressive signals produced by the EMP. The response time of the filtering technology is extremely short and energy absorption and shunting capabilities are extremely high. And the protection device continuously provides the rated voltage and current to the systems.

B. TEMPEST Prevention Design Guidelines

The prevention of TEMPEST problems can best be accomplished by being attentive to every stage of the computer systems design and development. And the most prevalent methods seem to be following RED/BLACK separation, shielding the equipment, filtering signals before they leave the facility, using proper grounding techniques, and using isolators on signal lines. RED/BLACK separation can reduce the RED possibilities of CE jumping on TEMPEST channels. Shielding keeps your signals inside an area, whether a computer case is any room. Filtering takes a set of signals in and usually only lets one signal out. Grounding or proper grounding with the path of least resistance for a conductor is to ground and not along the conductor away from your space.

Due to the many ways that information is processed in equipment, there are many ways that CE can be generated. It is nearly impossible to completely prevent the generation of such CE. Therefore, the TEMPEST design objectives should keep the amplitude and frequency spectrum of CE as low as possible below the limit, to prevent RED signals from coupling lines or circuits, and to prevent emanations from escaping from the systems through electromagnetic or acoustical radiation. And the whole defense in depth TEMPEST consideration is the design of equipment to meet TEMPEST requirements, the installation of infrastructure to maximize integrity, and the development of national security systems to utilize effective hardening strategies and hardware countermeasures.

Additionally, computer systems architecture should be designed by using TEMPEST tested to verify compatible with CE requirements. Other security countermeasures can be against compromising emanations, such as low emission laptops, effective software protection technique and a suitable jamming scheme as countermeasures against eavesdropping [18], [19].

VI. CONCLUSION

The important EMC problem related functional safety and emanations security to the computer systems architecture is electromagnetic security. The EME especially IEMI with the operation of equipment grows out of the electromagnetic effects on systems. Computer systems information leakage as TEMPEST problem may disclose emanations security from the sources which process plaintext and security data. There are some guidance to deal with EMC, to achieve electromagnetic security of computer architecture, and some defending methodology to control E3 damage and CE for information systems. A final note is that the implementation of comprehensive electromagnetic hardening would have a very interesting side effect, which being a substantial reduction of the levels of electromagnetic security risk for computer and networking equipment. The means and methods have been outlined, as have some defensive measures in an area which is bound to attract significant funding in the near future work.

REFERENCES


Changlin Zhou (IEEE, IACSIT) was born in 1961. He received the B.S degree in physical electron from Zhengzhou University in 1983 and the M.S. degree in communications and information systems from Zhengzhou information engineering university in 2005. He is an associate professor at Zhengzhou Information Engineering University. His research interests include EMC, circuit & systems design, computer security, system reliability analysis.

Qun Yu was born in 1981. He received the B.S degree and the M.S. degree in computer science and technology from Electric Engineering Institute in 2003 and 2007, respectively. He is a Ph.D candidate at Zhengzhou Information Science and Technology Institute. His research interests include electromagnetic protection, EMC.

Litao Wang was born in 1983. He received the M.S. degree in computer science and technology from Zhengzhou Information Science and Technology Institute in 2008. He is a Ph.D. candidate at Zhengzhou Information Science and Technology Institute. His research interests include information security, EMC.