Technical Guide

EAVESDROPPING PROTECTION

EMshield

an **Albatross Projects** company

Table of Contents

Preface

The threats of industrial espionage in general and bugging operation in particular are being discussed with high intensity in the recent years and these have become the topics for numerous surveys and publications.

While there are directives for bugging protection in the official sectors since many years, this topic is neglected in several companies despite the known threat situation. Instead of a coordinated, preventive approach, specific measures are adopted in most cases only in the event of damage. Often, the cause for this is the fact that there are no responsible persons for this subject area in the companies. Thus, bugging protection is frequently divided between IT security and classic security department. There is lack of expertise and human resources, in order to deal with this topic professionally. Considering the varied array of threats, this approach appears to be negligent.

The topic bugging protection is very complex. The specific implementation of safety measures requires experience in the security sector and technical knowledge not only in construction field, but primarily in the sector of high frequency technology. Professional projects are often handled by a team of specialists, e.g. a security adviser, internal safety department, architectural office and a speciality supplier for bugging-proof rooms. However, time and again, there has been a request from our customers and partners for a compact and generally understandable introduction to the subject. These guidelines address this request. These give an overview of the most important bugging operation approaches and corresponding safety measures. Initially, the possible threats are illustrated here with the help of practical examples. The second part gives an overview of the technical and structural safety measures.

Organizational measures are deliberately refrained from, since general recommendations cannot be given here without intensive security advice and knowledge of the organizational structures.

These guidelines should provide an introduction to the topic to the persons responsible for security in the company and authorities as well as to security advisers, who want to handle the topic bugging protection. Furthermore, we would like to assist with the selection of suitable bugging protection measures and with the development of security concept. Organizational and legal factor are marginally addressed here; however, these play a key role during the creation of such concept.

As a general rule: If the topic of bugging protection is considered while planning the location at an early stage, the measures can be implemented more efficiently and in a cost-effective manner. Thorough implementation of the recommendations from these guidelines and considering these as the basis for planning the new constructions would lead to a sound basis for bugging-proof environment.

Current threat situation

The expertise of German company – "Made in Germany" – is in demand across the world, even in foreign intelligence services and foreign competitors. Industrial espionage and competition espionage increasingly focus technology-oriented and innovative medium-sized companies - the backbone of German industry - in increasingly tough economic competition for products and sales markets. Many of these companies have very less knowledge about the risks of unintentional loss of expertise.

The business consultant Corporate Trust wants to raise awareness among these companies and hence it had published a survey on the topic "industrial spies" for the third time in 2014.

Results of this survey in brief:

- Every second company had complained about spy attack or suspicious cases in the past years. To be specific, 26.9 percent in Germany and 27.1 percent in Austria were affected by the particular event. Furthermore, 27.4 percent (Germany) and 19.5 percent (Austria) had at least one suspicious case. In Germany, this showed an increase by 5.5 percent as compared to the results from the survey in 2012. For Austria, the figures were collected for the first time.

- The yearly financial loss due to industrial espionage amounted to 11.8 billion euros in Germany and 1.6 billion euros in Austria. 300,000 companies in Germany and 42,000 companies in Austria were considered for calculating the loss. During the survey, only companies with more than 10 employees and with a revenue and total assets of more than 1 million euros were surveyed.

- 77.5 percent (Germany) and 75.0 percent (Austria) of the affected companies had reported financial loss due to spy attacks. The loss was between 10,000 and 100,000 euros for majority of the companies. Nevertheless, 4.5 percent (Germany) and 3.1 percent (Austria) had even complained about loss of over 1 million euros.

- Companies also suffered intangible losses due to industrial espionage; 37.1 percent in Germany and 30.5 percent in Austria were affected by it. Most common were patent infringements (Germany: 54.3 percent; Austria: 58.3 percent) and reputational damage with customers or suppliers (Germany: 26.8 percent; Austria: 22.2 percent).

- Mechanical engineering is again the most affected sector. 50 percent of all losses occurred in only three (Germany) and four (Austria) sectors. Automobile manufacture, aircraft construction, ship building and mechanical engineering were the most affected groups with 22.5 percent in Germany and 18.2 percent in Austria.

Which roles do bugging operations play?

According to the above mentioned survey2, approximately 10 % of the surveyed companies reported loss of information due to bugging of meetings. The estimated number is probably significantly higher, if it is assumed that not every bugging operation is noticed. A few spectacular cases, e.g. in the management board of Munich DIBAG3 or the publications of Mr. Snowden show e.g. the manifold potential threat.

Bugging protection is neglected

Despite manifest threat situation, the topic of bugging protection is not given sufficient importance. There are no responsible persons for this area in almost 60 % of the companies. Bugging protection measures play a minor role even in the topic building security. Only 7.5 % of the companies perform investigations for bugging devices on a regular basis4; only 4.1 % have bugging-proof rooms.

1) Refer to Corporate Trust (2014): "Survey: Industrial espionage. "Cybergeddon der deutschen Wirtschaft durch NSA & Co.?"
2) Refer to Corporate Trust (2014)
3) Refer P. 55
4) Refer to Corporate Trust (2014)

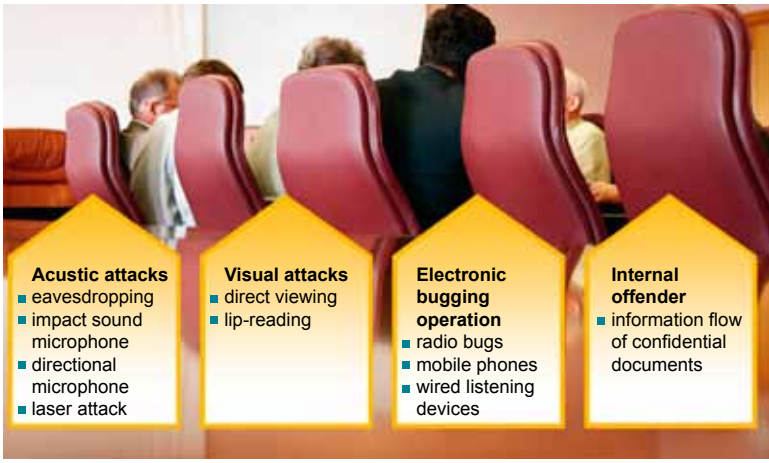

Figure 1: Possibilities for undesired information flow

Possibilities for undesired information flow

Figure 1 gives an overview of the different possibilities of attack. In addition to the technical possibilities, even banal threats such as direct viewing e.g. inside glass-enclosed conference rooms or the threat by internal offender are neglected.

Acoustic attacks

Sound waves, which arise during a discussion, set the components such as walls, ceilings and windows into vibrations. The vibrations continue even in heating pipes, air-conditioning ducts and sprinkler pipes. Modern laser microphones are based on interferometry and work in near-infrared range (NIR) at 790 nm or in the infrared range (IR) at 1500 nm. These can record discussions across several 100 m. Contrary to the conventional laser microphone, these search targets in the room (e.g. water glass, photo frame). Another acoustic attack possibility is a contact microphone, which is installed e.g. in the heating pipe. Thus, the discussions in the entire building can be monitored.
Technical aids such as these are not at all required in several cases. Many meeting rooms are not adequately insulated acoustically; thus, the discussions can also be monitored directly.

Visual attacks

Even if it seems elementary, we would like to point out here that confidential meetings must be protected against visual attacks such as direct viewing or lip-reading. Thus, the glass-enclosed meeting rooms designed with modern architecture are not suitable for confidential meetings. Even the option of conducting confidential meetings at external locations, e.g. in restaurants, park or at the airport lounge does not illustrate any professional information protection measure in this context. Basic prerequisite for a highly confidential meeting should be a closed and protected room.

Electronic bugging operation

Radio bugs

The perspective that the “bugging device” has been disused as listening device and has been removed through manipulation in the PC and digital telephone system is just partly correct. The fact is management floor and conference rooms can be accessed without any risks by trespassing the protocol settings of modern telecommunications systems or through installation of programs running in the background on the computer. The prerequisite here is the specialized knowledge and knowledge about internal structures of the bugging objective. For fast deployment, the conventional electronic listening device is still the preferred method. The current (almost) freely available listening devices are technically well-developed and have less resemblance with the classical “mini transmitter”: These no longer transmit information continuously, but save the information over some time and send it unnoticed within fraction of a second. These do not transmit at constant frequency, but change it from time to time. Many no longer have a distinctive radiofrequency carrier and can be hidden behind harmless transmitters (radio stations, private mobile radio etc.). Modern burst bugging devices emit short pulses and can be traced only with high-quality measuring devices and can be barely captured by a conventional measurement technology for anti-surveillance.

GSM bugging devices

The latest listening devices are GSM bugging devices, miniaturized mobile phones, which are also described as “Revolution in bugging technology”. This is because contrary to old, analogue bugging devices, in which the attacker had to be in the radio band of the bugging device (depending on the location of the object approx.1,000 – 5,000 m), the attacker can receive the information of GSM bugging device worldwide digitally and with the best voice quality. Since this listening device uses mobile radio frequencies, the bugging device is very difficult to locate. It is considered as the first choice being the fastest listening device with a price from approximately 30.00 €.

☐ Wired listening devices

The functionality of wired bugging device is comparable with a radio bug. The only difference is that the wired bugging device does not require external power supply, since it is simultaneously supplied with power via the manipulated line. The wired bugging devices can be used in all possible lines e.g. telephone or power cables.

☐ Manipulated mobile phone

Based on the modification of the mobile radio, it is no longer mandatory to install the electronic listening device in the premises. Modern mobile devices with Symbian Software can be manipulated using Software e.g. Flexispy that is freely available on Internet and these can be turned into bugging devices.[1] This can be done even without knowledge and support of the owner. If the Software is installed once, not only the mobile phone can be located, but also the telephone calls and room noise in the surrounding of the mobile handset can be intercepted. The phone number memory is readable for the attacker; transmitted and received short messages can be read and saved photos can be viewed. Furthermore, the mobile phone can be activated unnoticed via "silent call" and can be used similar to a bugging device for transmitting surrounding sounds. This works even in supposedly switched off state. The display goes out in manipulated device; however, the device remains operational. While it is important in these products to transfer the Software "manually" via interfaces such as Bluetooth or USB to the mobile handset, the threat due to mobile phone Trojan is discussed again and again.

According to a press release of the company Securstar, the mobile phone Trojan "RexSpy" programmed for demonstration purposes can be installed on a mobile phone with the help of an SMS, which the recipient does not notice and this can be turned into a bugging device. According to Securstar [2],

Figure 2: Scenario of eavesdropping operation via radio transmission

every average programmer can develop such Trojan with minimum effort. However, this is controversial among experts.

According to SPIEGEL Online [3], even German police use manipulated mobile phones to tap criminals. In the professional sector, it is always advisable to use an encrypted mobile phone.

1) e.g. www.flexispy.com/spyphone-bug-symbian.htmwww.neo-call.mobi/
2) www.securstar.de/press_2006_10_31.php
3) www.spiegel.de/netzwelt/tech/0,1518,494461,00.html

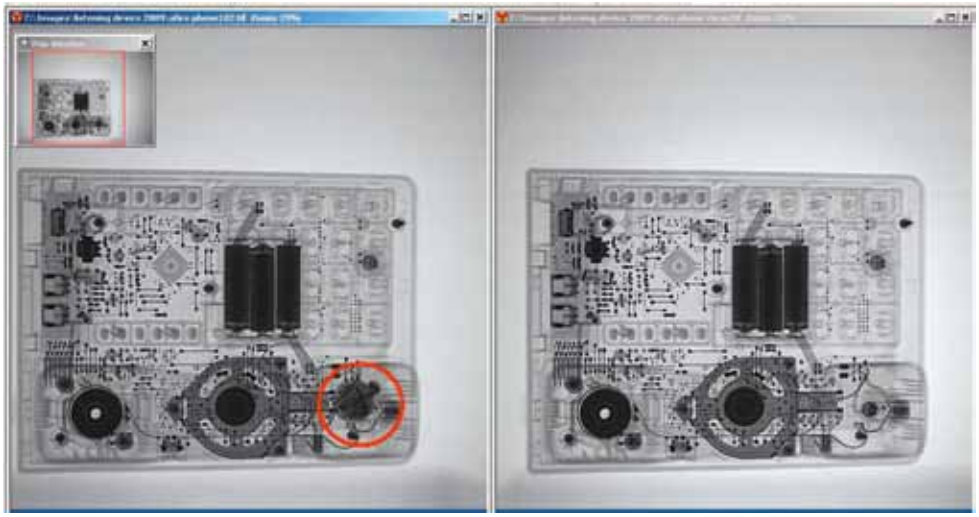

Figure 3:
Listening devices in telephone set

□ Manipulated telephone systems

Currently, the threat due to attack on telephone system is underestimated even in smaller companies. The maximum ISDN telephone systems remain in use with the default password. Only 20 % users take the effort to change the password after start-up of the telephone system. This situation opens way to buggingoperation. If the password is changedconstantly, this refers to significant protection, although this is not an insurmountable obstacle for a qualified hacker. Experiences from attack path analysis of reputed anti-surveillance companies show that it takes half an hour to one and half hour to crack the password.

It is more effective to install “Cerberus PCs”, i.e. a computer, which monitors and logs all settings and activities of the EC system without interruption. Most of the modern telephone systems have an interface for such “Cerberus-PC”.

However, even relatively simple protection considerations can be helpful for EC systems: thus, it should not be possible for remote maintenance to dial up, but the service technician calls up and sets a request for call back. The system then calls a previously programmed phone number, which has been carefully verified and checked beforehand.

Last but not the least, a possible manipulation of terminal devices (telephone and fax machine) should also be considered. Manipulated gravity hooks always appear in conventional telephones. Thereby, room noise is audible to the attacker even without accessing EC system software. In this case, only telephone and wiring analysers or mobile X-ray machines help. For this purpose, installation of a device of the same type in secured “clean” form is compared with device to be checked (see figure 3).

Voice-overIP (VoIP) is another topic in the context of manipulation of telephone systems; basically, VoIP is not unreliable than the conventional telephony service. In case of “landline” and mobile phones (GSM and UMTS-3G), the operators are legally bound to disclose the call detail records; currently, the internet providers do not have any legal obligation as yet. Thus, VoIP appears to be more “secure” than a conventional telephone, only as long as the attacker identifies the access option on VoIP server.

□ Compromising emanations/TEMPEST

Compromising emanations (even Compromising emissions or **compromising radiations)** refer to the electromagnetic emissions of technical devices, which allow conclusions on the data processed in the devices. Special receivers are required to evaluate these usually weak emissions. However, data such as the content of the computer screen can be analysed from up to 100 m distance through suitable measuring set-ups (with comparatively low costs). Datacentres for processing confidential data can be protected against undesirable loss of information either by low-radiating Hardware or by installing low-radiating areas (refer to page 12).

■ Internal offender

There is always a risk of information flow through an internal offender in all technical security measures. This risk must be handled with appropriate organizational measures. However, the threshold for internal offender also increases through implementation of technical security measures. Due to this reason, organizational aspects should always be considered while implementing the technical measures.

Protective measures against bugging

There are several options for protection against illegal information flow. These technical guidelines give secondary importance to the threat due to internal offender, since several social motives, organizational and personal issues may be involved here. The technical and organizational measures are inter-related due to the fact that technical safety measures also increase psychological barriers for internal offenders. There are simple safety measures for the area of visual attack. In most cases, interruption of direct eye contact is sufficient (blinds, privacy shield, jalousie, etc. – refer to page 4). There are two options for protections for the remaining two areas of acoustic and electronic attacks, which can be applied alternatively or additionally:

1. Technical counter surveillance measurement (TCSM)
2. Preventive structural measures

Active checks for anti-surveillance offer a high level of flexibility. These can be conducted even at short notice e.g. prior to a confidential meeting and in external facilities. However, these are snap-reading methods at the time of check and do not provide long-term protection. Long-term, sustainable protection is provided only with structural bugging protection measures. These structural measures require lengthy preparation and these should be considered in good time during the construction or renovation of the building. The protection through such structural measures is permanent and thus this is restricted to the respective room.

A combination of active and structural measures is recommended depending on the requirements for security and spatial and organizational conditions. The following section gives an overview of the different technical options and their applications.

Technical counter surveillance measurement (TCSM)

Active measures for anti-surveillance, i.e. sweeps refer to the checks of security areas with technical devices by specialists. This includes regular check of rooms for technical listening devices and accompanying continuous monitoring during a conference or meeting. To start with, several persons responsible for security face the issue, whether an external service provider is to be assigned with the check for anti-surveillance or whether the corresponding resources are to be arranged internally and provided with the necessary technical aid. External service providers help in quick implementation at lowest costs from short-term perspective.

However, set-up of an internal anti-surveillance is profitable not only in view of costs in the long term. Also, the security considerations should be noted while making decision regarding the protection of highly confidential information through an external service provider. Different devices and technologies for active anti-surveillance are presented below. However, a professional technical training is indispensable for correct application of the device.

Figure 4: Noise generator with the related transducers

Figure 5: Special spectrum analysers forchecks for anti-surveillance

Protection against acoustic attacks:

□ Noise masking and security film

Listening via laser systems or contact microphones can be inhibited with the help of sound-proof systems. The transducers installed on panes, in the walls and ceiling and in the pipes and the connected noise generator interfere the sound waves of the conversation with the randomly generated noise. The systems are set precisely with the relevant Software, so that it leads to minimum impairments in the room. It is recommended to apply laser protective filmsto the windows, in order to protect against penetrating laser beams.
An acoustical insulation can be integrated into the room architecture as an alternative or as a supplement (refer to page 12).

Protection against attacks via radio transmission

□ Detection of active transmitters

There are several options for protection against technical listening devices. An effective method is the use of intelligent test receivers. These are radio receiver / spectrum analysers, which cover a wide frequency band and which can detect and analyse the infra-red signals from air and long wave signals from power lines. Their analytical abilities are based on complex algorithms and high computing capacities, in order to locate the complex listening transmitters described above.

□ Applications for spectrum analysers

Such spectrum analysers can be used for basic examination of rooms and as conference room monitoring systems during confidential meeting. The systems are used as mobile systems with built-in batteries e.g. in meetings in external premises such as hotels or convention centres.

□ Detection of passive transmitters and semiconductor devices

Passive transmitters and semiconductor devices, such as listening devices, which currently do not transmit, or switched off mobile phones, are detected with a semiconductor detector or Non-Linear-Junction-Detector (NLJD).

A frequency in the range from 880 up to 2.4 GHz is emitted by means of a specially polarized antenna and the respective harmonic wave of this frequency is received. Harmonic waves are integral harmonious vibrations of source frequency, which occur during every wave movement. Thus, the second harmonic wave of 880 MHz is 1760 MHz (880 x 2) and the third harmonic wave 2640 MHz (880 x 3). If the radio wave emitted by the antenna of NLJD strikes an electronic component, then every semiconductor (transistor, diode, integrated circuit etc.) causes a strong reflection of the second harmonic wave. The semiconductor must not be always of electronic nature.

Even a door handle, which has not been operated over a long period of time, forms more or less good electrical (= semiconducting) transition between its moving metal surfaces. This corrosive transition causes strong reflection of the third harmonic wave. It can be reliably indicated from the relation of second and third harmonic waves shown on the display of NLJD, whether it concerns a threat due to electronic listening devices in the wall or is it a part of rusty structural steel in the concrete.

□ Applications of Non Linear Junction Detectors (NLJD)

NLJD is sensibly used in such cases, if the basic examination of the room has been conducted and a current threat due to electronic listening devices is expected. A modern NLJD is an important tool in the course of a professional room check (“sweep”).

□ Checking of network-, telephone and power lines

If the rooms are examined for active transmitters and semiconductor devices, then the lines, which are laid in the room, present security-relevant problem. In order to fill these gaps, all lines are measured and checked with the appropriate measuring devices. The following devices are required for such check: Multimeter, audio amplifier, power distribution system, time-domain reflectometer, digital audio demodulator and oscilloscope. In recent times, even multifunctional devices such as the wiring analyser TALAN formulated specifically for this application have been used, which cover the entire functionality. This device combines the necessary functions into one and furthermore offers detection of listening devices in lines with the frequency domain reflexometer measurement. TALAN has 80 % of the worldwide available ISDN protocols and can rectify these.

Figure 6: Line analyser TALAN

□ Application of line analysers

Such multifunctional line analysers automatically check all electrical lines in the office or meeting rooms for listening devices. The properties of rooms are saved with the corresponding Software and this is again called at a later point of time. Thus, the repeated checks can be conducted fast and in an efficient manner.

Figure 7: Non-Linear-Junction-Detector in use

Structural protection measures

Structural measures provide long-term protection contrary to the active safety measures, which is a snap-reading method. Structural measures can be implemented in new constructions as well as in the existing buildings. This also refers to bugging-protected rooms or radiation protected rooms. Such areas protect against external attacks and increase the psychological barrier for internal offenders.

■ Bugging-protected rooms

Bugging-protected rooms refer to structural strengthening (shielding) of a room, in order to prohibit bugging of information by means of acoustic, visual and electronictransmissions. The main feature of bugging-protected and bugging-proof rooms is that any kind of high-frequency transmission e.g. through mobile phone, bugging devices, WLAN, etc. is interrupted by electromagnetic shielding. All lines (power, telephone, etc.) are directed through special filters to the room, whereby even wired transmission is prohibited. This is achieved by construction of a Faraday cage (electromagnetic shield). More detailed information on the principle of electromagnetic shield in available in our “design manual - electromagnetic shield”.

This shield can be supplemented by acoustical insulation, laser protective film, privacy measures and other safety measures such as access control. Bugging-protected areas are provided at locations, wherein one may want to create fallback areas in the long-term for confidential meetings, e.g. meeting areas of the management in companies or for secret meetings in official sectors. There is a distinction between bugging-proof and bugging-protected areas.

□ User acceptance

User acceptance is crucial for the success of bugging protection measures according to our long years of experience. If a bugging-proof area in the form of a room within a room system without windows is installed e.g. in the basement of the registered office, which even fulfils the high requirements for bugging safety, then the probability is that this room is used by top management with zero trend. With modern shielding technologies, even completely normal meeting areas can be reliably protected against bugging operations, without the comfort being markedly affected. Such shielding is optically barely recognizable to laymen. These rooms have high acceptance from the users and are used intensively.

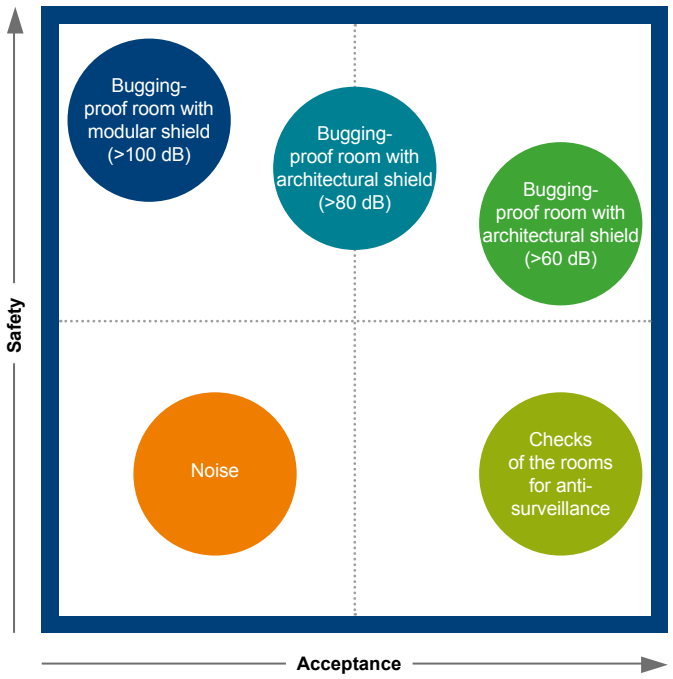

Figure 8: Schematic representation security and user acceptance of bugging protection measures

This interrelation between security requirements, comfort and user acceptance should be considered during installation of bugging-protected areas and the appropriate solution must be selected.

A bugging-protected area is integrated in the existing or newly emerging buildings, without the user being subjected to significant restrictions – the user does not notice that he is in a shielded room.

However, a bugging-protected area can be installed in a new construction or during renovation with considerably less effort and significantly lower costs than in an existing building.

The bugging-protected area should be considered in planning at an early stage. Our checklist “bugging-protected room” helps with the selection of suitable rooms. We will be happy to provide this checklist upon request.

Requirements for bugging-protected and bugging-proof rooms

	Bugging-protected room 60 dB	Bugging-protected room 80 dB	Bugging-protected room in accordance with BSI requirements100 dB
Requirements for safety	Standard	High	High requirements in official sector
Electromagnetic attenuation of shielding	60 dB 30 MHz - 10 GHz	80 dB 30 MHz - 10 GHz	100 dB 30 MHz - 10 GHz
Acoustical insulation	45 dB (A), optional 52 dB (A)	45 dB (A), optional 52 dB (A)	Prescribed: 52 dB (A)
Material	EMshield Shielding Material/ fleece	EMshield Shielding Material	Prefabricated steel sheets
Equipment/ interior design	No restriction in the architectural design of the room (windows, glass facades, standard doors, etc.)	Limited selection of shielded windows	No windows possible; design with defined shield components possible; access through security gates

Low-radiating and radiation-proof areas/ TEMPEST / EMP-HPM

Low-radiating and radiation-proof rooms refer to structural strengthening (shielding) of a room, in order to prohibit dispersal of compromising radiations tothe surface. These rooms inhibit the high frequency radiation from computers, printers and connected peripherals. These radiations are known as compromising radiations. Compromising radiations are thus to be differentiated from electromagnetic compatibility, which deals with mutual impact of devices due to electromagnetic fields. The thresholds for electromagnetic compatibility are not sufficient to prevent compromising radiations.

Due to this reason, the computers, on which sensitive data such as certification authorities for Public-Key Infrastructures (PKI) is processed, are located in low-radiating and radiation-proof areas. The location of the room and factors such as options of access control etc. are crucial for determination of emission protection. In this regard, the zone model of Federal Office for Information Security (BSI) is concerned. BSI is a civil higher German Federal authority in Bonn in the business area of Federal Ministry of the Interior (BMI), which is responsible for queries related to IT security, bugging and radiation protection for companies involved in industrial security.

□ NATO Zoning

The zone model should ensure that analysable radiations are not detected in publicly accessible areas that are susceptible to bugging attack.1 Thus, the zone model considers the dispersion conditions for compromising radiations for the respective building and surface conditions. These conditions are measured and recorded, in which the weakening (room and free space loss) of radiations through physical obstacles in their path is measured from the inducing IT device to the potential recipient. An optimum level of radiation safety is achieved at minimized expense in this manner. The zone model can be applied only to buildings and properties as well as stationary used mobile devices, for which a precisely definable range limit outside the building can be set.

1) Refer to: BSI: Technical guidelines: Electromagnetic shield of buildings – Theoretical Basics –, P. 23.

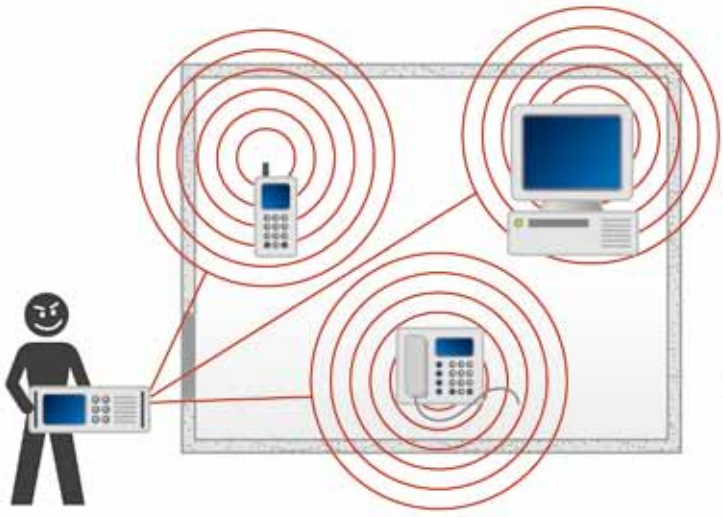

Figure 9a: Electromagnetic emission of technical devices can be received from outside in unshielded rooms.

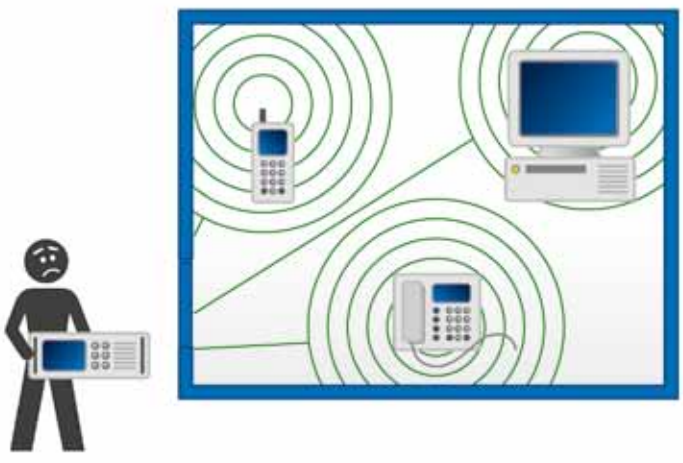

Figure 9b: Shielded rooms protect against bugging operations.

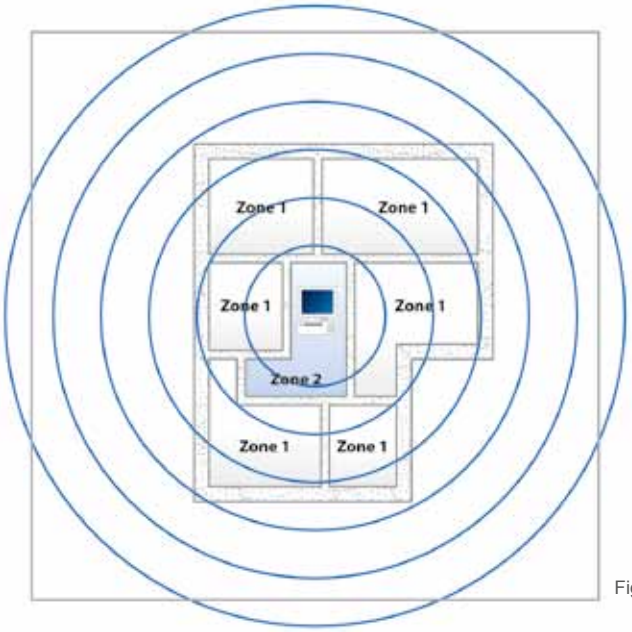

Figure 10: Schematic representation of BSI zone model

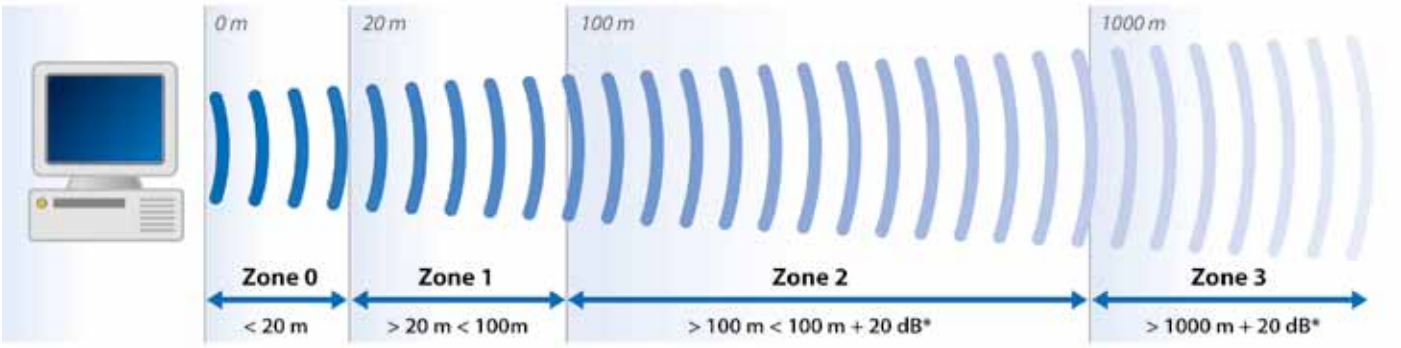

Figure 11: Overview of zonation BSI zone model (*20 dB correspond to approximately tenfold increase)

Individual floors or rooms within the buildings cannot be "zoned" opposite to other floors or rooms, i.e. classified. In such areas, bugging-proof or radiation-proof rooms must be constructed.

□ EMP-HPM protection

Contrary to radiation-proof rooms, it comes down to protection of computers against electromagnetic pulses from outside (radiation protection) in case of protection against EMP-HPM. Electromagnetic shielded rooms are used even in this case (e.g. datacentre, critical infra-structures, etc.)

□ Radiation-proof rooms in accordance with BSI requirements:

Please contact BSI for requirements for radiation-proof areas:

BSI Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] Godesberger Allee 183–185
53133 Bonn
Tel.: 0228 999582-0
www.bsi.bund.de

Electromagnetic shielding: This is how it works

Radio signals such as mobile telephony, radar, Wireless LAN are transmitted in the form of electromagnetic waves. These electromagnetic waves can be shielded through a Faraday cage. A Faraday cage is a jacket made of electrical conductor closed from all sides (e.g. wire mesh or sheet metal). All elements of the shield must be interconnected in completely conductive manner.

The effectiveness of shielding measures is denoted as electromagnetic attenuation of shielding and this is specified in the unit dB.

The shield factor S of shielding is defined as the ratio of unshielded to shielded radiant power. A logarithmic representation is selected, since this ratio can take wide value range in case of real materials, almost 1:1 for poorly shielding materials (0 dB), 1:1000 for good shielding (60 dB).

The attenuation of shielding SESE is thusdefined as the logarithmic ratio of incident radiant power without shield to incident radiant power with shield. The unit of attenuation of shielding is Decibel [dB].

Attenuation of shielding is a dimensionless measured variable, which quantifies the effectivity of shielding.

While shielding is a technical measure, attenuation of shielding is a measure for the quality of a shield in electromagnetic compatibility. According to the principle of Faraday cage, the shield plays the role of a space, which it encloses to protect against external electric field; its effectivity is recorded with attenuation of shielding. Attenuation of shielding also describes the protective effect against the magnetic field and the electromagnetic field. Attenuation of shielding is often specified even in case of shielded lines. The usual, technically unique measured variable for recording the shielding effect of a line corresponds to transfer impedance or antiquates coupling resistance. MIL-STD 285, the military standards regarding defence equipment VG 95370, Part 15, or US Standard NSA 65-6 define common measuring techniques for attenuation of shielding. MIL-STD 285 has been replaced in 1997 by IEEE-STD 299.

Dezibel (dB) is not a unit such as Volt, Ampere or Watt, but it is a ratio. For figures with the unit dB, a ratio has been set between two other figures beforehand. It is a mathematical specification, which alone is not significant. Thus, it must also be included for dB specification, as to what it indicates. In order to effectively shield a room, it must be enclosed by a closed, electrically conductive jacket. Holes, slots or objects penetrating the jacket destroy the shielding effect. Thus, it does not make any sense to shield the walls with the help of copper wallpaper, if the windows, doors or lines are not shielded.

Link between the Decibel values and % values for U, E, H, P and S

dB values strengthpower density	Penetrating voltage or field	Penetrating power or	Shielded power
0 dB	100 %	100 %	0 %
10 dB	31,6 %	10 %	90 %
20 dB	10 %	1 %	99 %
30 dB	3,16 %	0,1 %	99,9 %
40 dB	1 %	0,01 %	99,99 %
50 dB	0,316 %	0,001 %	99,999 %
60 dB	0,1 %	0,0001 %	99,9999 %
80 dB	0,01 %	0,000001 %	99,999999 %
100 dB	0,001 %	0,00000001 %	99,99999999 %

There are different materials for surface shielding of electromagnetic radiations, the attenuation properties of which are of very different grades. The individual components alone do not ensure effective protection. The **system** is decisive. The complete shielding of a room can be implemented, only if compatible components are used. Thus, optimal protection can be ensured. Different systems have been established for room shielding depending on the requirements for security and architectural design:

□ Architectural room shielding

Architectural room shielding systems are systems, in which all components are integrated into the existing room architecture and thus the natural atmosphere of the room is retained. In addition to surface shielding, all components such as windows, doors, ventilation, lines etc. are provided with corresponding shielding. This shielding is barely recognizable to laymen from outside. Architects and planners will have the greatest possible freedom. The surface shielding is provided here with copper pyrites or with thin copper sheet. Thus, the shielding system can be re-treated e.g. with all conventional flooring and wall materials. Air conditioning, electrical installations and media technology can be integrated according to the requirement. Detailed information regarding all components of such system is available in the data sheets for EMshield system.

Shielding attenuation levels of > 80 dB can be achieved with guarantee with architectural room shielding systems. Architectural shielding systems can be integrated into new constructions and existing rooms. These are permitted for permanent workstations, so that even rooms with windows can be shielded.

□ Shielded chambers/ modular shielding

Shielded chambers made of copper or steel sheet modules are used for high requirements of safety and electromagnetic attenuation of shielding. Shielding attenuation levels of > 100 dB can be thus ensured. The options for architectural design are significantly restricted here. These chambers are provided as room within room. Windows are not possible. The selection of doors and wall and floor coverings is restricted. These systems are used in high security zones in official sectors.

Detailed information regarding electromagnetic room shielding is available in our “design manual - electromagnetic shield”; this shall be provided by us upon request.

Figure 12: Architecturally shielded room

Figure 13: High-security area with modular shielding

Summary

Listening device	Transmission	Possible countermeasures
Directional microphone	Acoustic	Acoustical insulation, noise by means of noise generators, use of rooms within the buildings
Listening	Acoustic	Acoustical insulation, access control
Contact microphone	Acoustic/ electronic	Acoustical insulation and/or electromagnetic shield, ORION (planned search for listening devices with special equipment)
Video-/photo monitoring, if required, with lip reading	Optical	Darkening of panes (blinds), use of rooms inside the buildings
Laser attack: Glass panes are displaced by sound waves in vibrations while speaking. In case of visual contact (e.g. from adjacent buildings), a laser beam can be directed towards these reflecting surfaces and the reflected beams are received again. The reflected beam is modulated by vibrations. The conversation can be made audible through demodulation.	Acoustic	Use of rooms inside the buildings (blinds on the outside), use of rooms inside the buildings, noise of panes, installation of laser protective film TR 70 on the glass
Mini transmitter, Audio, Video	Electronic	Electromagnetic shield, OSCOR, ORION
Microphone with transmission via fixed cables, communication cable, antenna cable etc. Even water pipes come into consideration	Electronic	Electromagnetic shield (incl. filtration), TALAN, ORION
Microphone with transmission via power supply system	Electronic	Electromagnetic shield (incl. filtration), TALAN
Manipulated landline telephone, fax devices or telephone systems	Electronic	Removal of EC-facilities in case of safety-relevant discussions, check of EC-facilities for manipulation, TALAN
Manipulated mobile phones or cordless telephones (the latter must never be manipulated for audio monitoring)	Electronic	Removal of EC-facilities in case of safety-relevant discussions, electromagnetic shield, OSCOR
Wireless intercom or microphone systems (manipulation is often not required even here)	Electronic	Removal of facilities in case of safety-relevant discussions, electromagnetic shield
Compromising radiations	Electronic	Electromagnetic shield, use of special low-radiating device

Check list/ specifications/ tender specification

We support in planning and advertising your individual shielding project completely and professionally. With the help of our checklist spatial recording, you can start detailed quote request for your project with minimal time requirement.

The specifications for doors and windows substantia-teyour request and are used for creating design and construction documentation.

Standards/ references

[DIN 4102 04]
Fire behaviour of construction materials and components, Parts 1 to 22, 2004

[DIN 18230 02]
Structural fire protection in industrial buildings, Parts 1 to 3, 2002

[DIN EN 50147-1 96]
Absorber lined chamber part 1: Shielding effectiveness measurement;
German Version EN 50147-1:1996, 1996

[EMVG 98]
Law on the electromagnetic compatibility of devices, 1998

[IEEE 299 97]
IEEE Std 299, 1997

[MIL 285 56]
“Attenuation Measurements for Enclosures, Electromagnetic Shielding, for Electronic Test Purposes, Method of”, MIL-Std-285, US Dept. Of Defence, 1956

BSI (2007):
Technical guidelines: Electromagnetic shield of buildings (BSI TR-03209)

EMshield (2014):
Design manual “Electromagnetic shield”

EMshield

an **Albatross Projects** company

Technopark I
Bretonischer Ring 12
85630 Grasbrunn / München

Tel: +49 (0)89 45 45 482-0
Fax: +49 (0)89 45 45 482-28

Email: info@emshield.de
Web: www.emshield.de