

SCIFs - State of the Art and Future Considerations

diyscif

May28, 2021

Abstract

This paper will examine the different constructive and technical measures employed by governmental, non-governmental, and corporate actors to protect their secret communications in the physical realm. It will define the target ideal state of “information security”, identify information sources that must be controlled to reach this state, set up quantitative limits on these information sources discoverable externally, provide example attack techniques, and propose various passive and active countermeasures to reach these limits and defend against these attacks. Finally it will present an example module that achieves these specifications measurably.

Note, this paper is limited in scope to constructive and technical measures and does not focus on IT or organisational security measures, like encryption, security-related review/monitoring of employees, and classification levels. It also does not dwell on specific countries bureaucratic protocols, but instead aims to present a unified picture of the global state of the art.

Contents

1	What is a SCIF?	2
2	Information Security - Ideal State and Practical Tradeoffs	3
3	Passive Outside Observer	4
3.1	Visual	4
3.2	Acoustic	5
3.3	Electromagnetic/TEMPEST	6
4	Limits	7
4.1	Visual	7
4.2	Acoustic	7
4.3	Electromagnetic/TEMPEST	9

5	Active Attacker	10
5.1	Visual	11
5.2	Acoustic	11
5.3	Electromagnetic/TEMPEST	12
6	Countermeasures	13
6.1	Physical	13
6.1.1	Construction Security	13
6.1.2	Intrusion Resistance	16
6.1.3	Intrusion Detection System	18
6.1.4	Access Control	21
6.1.5	Locks	22
6.1.6	CCTV	23
6.2	Visual	24
6.3	Acoustic	24
6.3.1	Sound Attenuation	25
6.3.2	Sound Masking	29
6.3.3	Microphone Jamming	31
6.4	Electromagnetic/TEMPEST Shielding	32
6.4.1	Functional Principles	32
6.4.2	Materials	35
6.4.3	Joints and Gaskets	37
6.4.4	Penetrations	38
6.4.5	Safety	40
6.4.6	Shielding System Function Monitoring	40
6.4.7	Signal Jamming	41
6.5	Bug Sweeping	42
7	Example Module	42
7.1	Physical	42
7.2	Visual	42
7.3	Sound	42
7.4	Electromagnetic/TEMPEST	42
	References	42

1 What is a SCIF?

Sensitive compartmented information facility (SCIF) is a term used by U.S. military and intelligence organizations to describe secure, enclosed areas designated for handling sensitive, classified information. They come in many different shapes and sizes, each designed for a specific mission demand. They can be installed permanently in buildings, designed as mobile units, set up temporarily, and even built aboard aircraft and naval vessels. What unites these different variants is the common goal of creating a designated space with rigorous security

practices that thwarts all relevant passive outside observers and active attackers.

SCIFs are by no means exclusive to U.S. government institutions. They are used internationally by a wide variety of actors, from other governments to international organizations to corporations and NGOs. The term has become the most commonly used and will also be used in this paper to refer to structures specifically built to protect information processed inside them.

Most countries keep their specifications for these secure facilities secret. The United States, however, have published comprehensive information on their engineering practices under Intelligence Community Directive (ICD) 705 “Sensitive Compartmented Information Facilities” and its associated technical specifications. In this paper, ICD 705 will be supplemented by private contractors’ informational material, documents released under the Freedom of Information Act (FOIA), leaked documents, and scientific literature to create a comprehensive picture of the current state of the art and give an outlook on future improvements.

2 Information Security - Ideal State and Practical Tradeoffs

A communication link or room is considered secure if information travelling through it cannot be intercepted by unauthorized parties. This is a theoretical ideal state that *cannot* be reached. However, one can employ various countermeasures to secure a communication link or room to such a degree that it can be practically considered as secure against an attacker with certain resources.

Both defenders and attackers are constrained by limited resources. Viewing attack techniques from a resource perspective allows a defender to determine whether they are “in scope”, given the threat level, and if countermeasures must be deployed against them. Resources are best expressed in terms of cost, time, and technical skill required. Taking into account these parameters, the defender is able to develop a mission-specific threat model that allows him to employ his *limited* resources effectively to defend against the most likely and serious attacks.

The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, p. 20) bases its threat modelling on country-level threat ratings derived from the Department of State’s (DoS) Security Environment Threat List (SETL). Specifically, the ICD establishes appropriate construction criteria based on the host country’s SETL technical threat rating. A country-level view is most useful to government organizations, however, other actors, especially corporate actors, may have to rely on different factors to determine threat level. Other possible criteria from which to derive a threat level include value of information handled and named/identified threats.

The fundamental assumption for threat modelling is that it is highly unlikely for an attacker to expend more resources to carry out an attack than the objective value of the attainable information.

3 Passive Outside Observer

There are various information sources that can leak from the secure facility and be intercepted. These can generally be grouped into visual, acoustic, and electromagnetic information source leaks. A passive observer can use different sensors, like telescopic cameras, directional microphones, and high-sensitivity antennae, to capture and analyze these information source leaks and draw conclusions about the sensitive information processed. A covert location outside the SCIF perimeter is almost impossible to detect and counteract. Therefore, information leaks must be prevented at the source.

3.1 Visual

Visual leaks are any direct view of sensitive information or surface whose reverberations can be captured with a laser and then translated into usable information. When speaking, glass panes or mirrors in a room are set into vibration. When there is visual insight into the room (e.g. from the neighboring building), a laser beam can be directed onto these reflecting surfaces and the reflected beam can be received again. The reflected beam is modulated by the oscillations. By demodulation, the conversation can be made audible (Wolfsperger 2008, p. 463). Direct views can also provide valuable insights into information processed and even serve as a basis for other attacks, like lip-reading of sensitive discussions.

Barring holes in the SCIF perimeter, like propped-open doors, visual leaks can only be captured through windows.



Figure 1: Laser Microphone Sptectra M+

Capture Technique	Cost	Time	Technical Skill Required
Direct View	medium	low	low
Lip Reading	medium	low	medium
Reverberations Captured by Laser	high	low	medium

3.2 Acoustic

Acoustic leaks are sound waves that escape the enclosed areas, either directly or through structure-borne sound transmission. These can be captured with directional microphones, contact microphones, and well placed conventional microphones. An example of such an advantageous placement would be in an unmuffled ventilation or heating duct.

Acoustic leaks provide some of the most valuable insights. Discussions, conferences, and chatter contain secrets in their purest form. Through them, an attacker doesn't only attain sensitive material, he also gains insight into underlying priorities and considerations, much more so than from a leaked document. Like Christoph Waltz's character from the 2009 Quentin Tarantino film "Inglourious Basterds" says "I love rumors! Facts can be so misleading, where rumors, true or false, are often revealing."



Figure 2: Parabolic Microphone G-PKS PRO EX

Digital sound processing software can further enhance an outside passive attackers capabilities to reconstruct, clarify, and analyze sound leaks.

Capture Technique	Cost	Time	Technical Skill Required
Directional Microphones	medium	low	low
Contact Microphones	low	medium	medium

Capture Technique	Cost	Time	Technical Skill Required
Conventional Microphones	low	medium	medium

3.3 Electromagnetic/TEMPEST

Compromising electromagnetic waves unintentionally emitted from information processing equipment, like computers, screens, and even printers are another source for information leaks. These radio or electrical signals, sounds, and vibrations can be captured with antennae, microphones, and other sensors, and allow inferences to be made about the information processed, sometimes even allowing its complete reconstruction (Liu, Samwel, Weissbart, Zhao, Lauret, Batina, Larson 2020). They can also serve as a side-channel for attacks on cryptography (Genkin, Pachmanov, Pipman, Tromer 2015). The techniques for extraction and analysis of compromising electromagnetic emanations fall under the commonly used U.S. National Security Agency codename TEMPEST (U.S. National Security Agency 1972).

These attack techniques require high technical skill to develop, however once established are easy and fast to reproduce with [affordable equipment](#). Although execution is fast, reconnaissance, planning and setup, especially for well-protected facilities, can entail significant time expenditure.

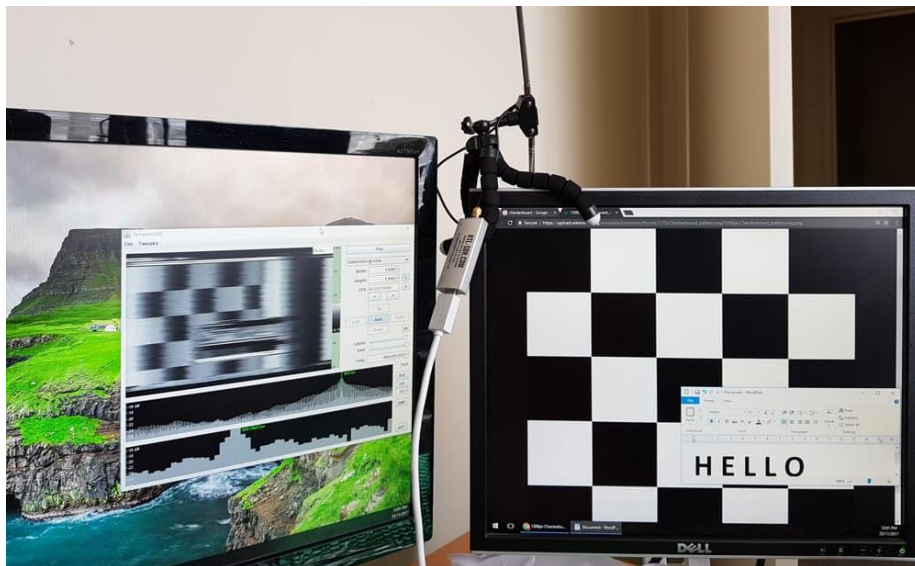


Figure 3: Display of one monitor reproduced on another using its TEMPEST emanations and a \$40 software defined radio + antenna set up. RTL-SDR.com (2017)

Capture Technique	Cost	Time	Technical Skill Required
Direct Leaks	low	medium	high
Side-channel on Cryptography	low	medium	high

4 Limits

This section will set quantitative limits on information sources available to an outside passive observer. Since information source leaks must be protected at the source, it is important to know the extent of attenuation necessary to assure adequate protection.

4.1 Visual

No visual information should be accessible to an outside passive observer. Visual information source leaks are the easiest to avoid and should therefore be wholly prevented. Even observation of the entrypoint could provide insights into the comings and goings of authorized personnel and should therefore be obscured as much as possible.

4.2 Acoustic

Acoustic emissions must be reduced by at least a weighted sound reduction index of $R'_w = 52$ dB. This measure roughly corresponds to the Sound Transmission Class 50 listed in the IC Tech Spec-for ICD/ICS 705 as an enhanced rating for areas that provide for amplified conversations (Office of the National Counterintelligence Executive 2012, p. 66). We use this as a general minimum measure, because the IC Tech Spec is geared towards military and other government facilities that provide a large measure of Security in Depth (SID), meaning that only semi-trusted personnel ever get within earshot of the SCIF. Security in Depth is a “multilayered approach, which effectively employs human and other physical security measures [like fences, walls, and guarded entry gates] throughout the installation or facility to create a layered defense against potential threats” (Naval Facilities Engineering Systems Command Northwest 2012, p. 20). Additionally, SID increases the probability of detection of nefarious activity because of continuous friendly-forces presence (Office of the National Counterintelligence Executive 2012, p. 3). These conditions cannot be guaranteed for all locations, especially in the corporate realm, so we strive to compensate reduced SID with a higher degree of sound insulation. When possible, $R'_w = 52$ dB should be exceeded.

R'_w represents the resulting sound insulation between two rooms, taking into account all sound transmission paths (Tichelmann, Pfau 2000, p. 26). This explicitly includes not only transmission through dividing components, but also so-called “flank transmission” over adjoining building components. In this phenomenon sound waves cause vibrations in flanking walls and then linearly travel

through them into the other room (Möser 2009, p. 254). R'_w is a cumulative value calculated on the basis of the weighted sound reduction index of each component R_w (Tichelmann, Pfau 2000, p. 34).

R_w is calculated by measuring sound transmission from one test cabin into another divided by the test component. The test is carried out in one-third octave or octave steps. White noise, a random signal with equal intensity across different frequencies, with the given bandwidth is used as test sound. A frequency response curve R is thus obtained in the so-called building-acoustics frequency range between 100 Hz and 3.15 kHz. The frequency response curve R is then compared to a reference curve B in order to derive a single comparison value. In the comparison, the reference curve is shifted in 1 dB steps onto the frequency response curve until the sum of the undershoots S_U of the frequency response curve compared to the reference curve is less than 32 dB. (Möser 2009, pp. 256–257)

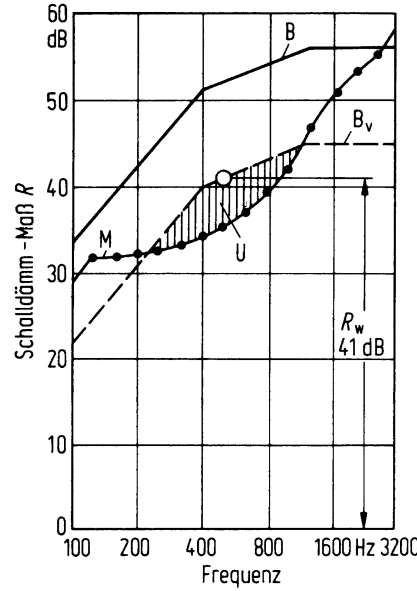


Figure 4: For the definition of the weighted sound reduction index R_w . B = Reference curve, B_v = Shifted reference curve, M = Measured values, U = Undershoots of M compared to B_v . Gösele, Schröder (2004)

From this diagram we can also see that for a $R_w = 52$ dB (the reference curve) the fundamental frequency of the male voice - 125 Hz - only undergoes a sound attenuation of ca. 35 dB. Given a 60 dB conversation sound-level the sound attenuation is not sufficient to protect from a close proximity attacker. Passive sound-attenuation measures should be specifically evaluated in the 125 Hz to 300 Hz range, and significantly exceed the reference curve's performance.

Airborne sound transmission via ventilation and structure-borne sound transmission via ducts, such as water and ventilation pipes, can significantly reduce sound insulation (Deutsches Institut für Normung 2018, p. 19). In some cases they can even provide direct channels for an outside observer to capture sound on (Office of the National Counterintelligence Executive 2012, p. 13). Hence, they must be treated with special attention. A mistake on a component penetrating the SCIF perimeter, like a duct or vent, can render useless all other attenuation.

4.3 Electromagnetic/TEMPEST

Electromagnetic emissions should be reduced by the values defined in National Security Specification for Shielded Enclosures NSA 94-106. This specification sets forth an attenuation for a 1 kHz - 1 MHz H (magnetic) Field of 20 dB @ 1kHz, 56 dB @ 10 kHz 90 dB @ 100 kHz, and 100 dB @ 1 MHz. For a 1 kHz - 10 MHz E (electromagnetic) Field it requires 70 dB @ 1kHz, and 100 dB at 10 kHz, 100 kHz, 1 MHz, and 10 MHz. For a 100 MHz - 10 GHz Plane Wave it also requires 100 dB attenuation.

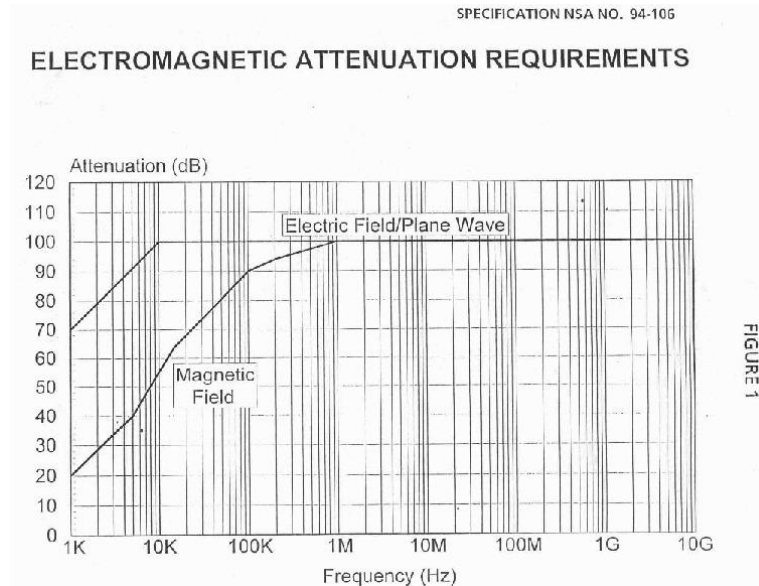


Figure 5: Electromagnetic Attenuation Requirements. U.S. National Security Agency (1994)

The field test is carried out with a parallel setup. A continuous wave source generates a wave in the range of 1 KHz to 10 GHz. Two antennae are placed, one on either side of the shielding. One antenna acts as a transmitting (TX) antenna and the other as a receiving (RX) antenna. The antennae are separated by a distance of 61 centimeters plus the wall thickness. The signal from the

RX antenna is fed back into a receiver. Attenuation levels can then be read from a spectrum analyzer. Magnetic field, electronic field, and plane wave attenuations are then measured at various specified frequencies. Attenuation tests are performed around the entire door frame, air ducts, filters and through any accessible joint or penetration. (U.S. National Security Agency 1994)

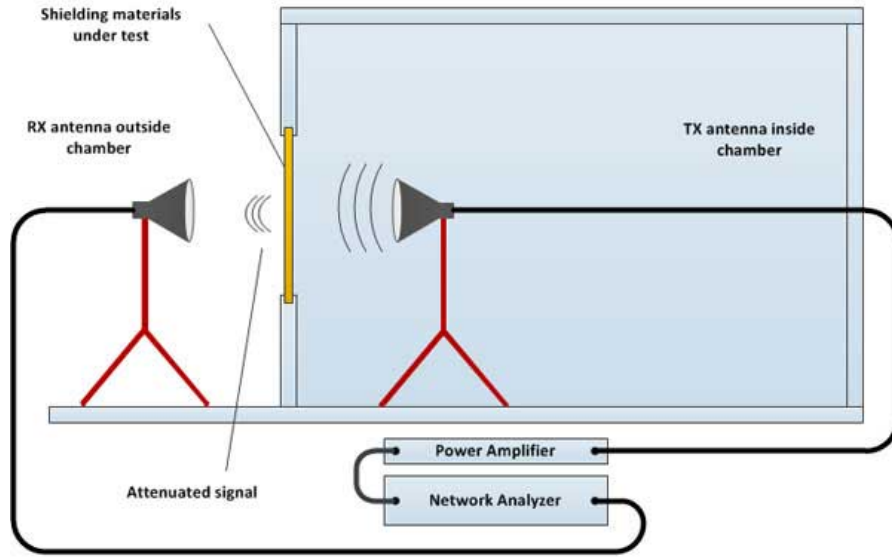


Figure 6: Test setup for NSA-94-106. EMCTEST Technologies (2018)

A RF shielding system is only as effective as its weakest component (Krieger Products 2015). Shielding material faults and gaps in the shield should be carefully avoided. These holes become more critical the higher the frequency of the shielded field (Wolfsperger 2008, pp. 292–293).

Apart from airborne electromagnetic waves, emanations can also leak from a SCIF on cables and wires. Instead of travelling through the air, unwanted signals can travel along wires out of the SCIF (Wolfsperger 2008, p. 210) inducing electromagnetic fields where they can be captured and turned into usable intelligence. With the right setup using different tools for power, data, and control connections these information source leaks can be entirely eliminated.

5 Active Attacker

Apart from passively observing information source leaks from outside the secure facility, an attacker can also actively attack the space to place sensors inside the SCIF and transmit sensitive visual, acoustic, or electromagnetic information

to the outside. He can also seek to weaken the passive attenuation in order to increase the information yield of passive observance.

This chapter intends to give some general ideas about possible attack vectors, not to list out specific attacks and describe their execution. New attack methods are constantly being developed and only few ever get published. Thankfully most can be prevented by sticking to the same established general countersurveillance measures and security practices.

5.1 Visual

The goal of all visual attacks is to place cameras inside the SCIF. These cameras allow an attacker to gain valuable insights into the sensitive information being handled or processed inside the enclosed area. Cameras can be inserted by someone who gains physical access to the space, inserted through HVAC ducts, or drilled through the perimeter.

Another attack avenue is taking over installed CCTV cameras. The video feed from these cameras could allow insights into the SCIF's comings and goings, and, with badly placed cameras, even into the information processed. This attack can also target the built-in cameras of information processing equipment like laptops.

Cameras transmit video feeds to the outside using radio/electromagnetic waves or wired connections. Wired connections could be specially installed for the attack or hijack existing lines, either directly or as emanations along their unshielded exterior.

Attack Technique	Cost	Time	Technical Skill Required
Inserting Camera	low	low	medium
Hijacking Existing Camera	low	medium	high

5.2 Acoustic

An attacker may also attempt to place a microphone in the SCIF. To do this he can either physically insert a new microphone or hijack one of the built-in microphones of devices already located in the room. Acoustic information is usually most sensitive, especially in conference rooms or discussion areas.

Similar to visual attacks, avenues for placing a microphone are physical entry, HVAC ducts, and hole drilling. In order to exfiltrate information the attacker again utilizes either radio/electromagnetic waves or wired connections, existing or specially placed. Another attack is finding a weak spot in the sound attenuating shell and placing a contact microphone directly on it.

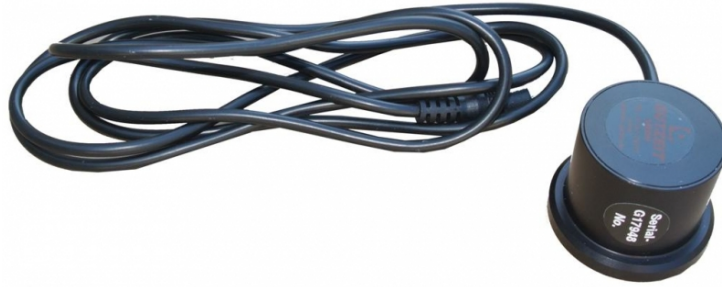


Figure 7: Contact Microphone Gutzeit GmbH

An attacker could also seek to weaken the sound attenuation measures by tampering with the sound masking, destroying insulation or purposely creating sound bridges.

Attack Technique	Cost	Time	Technical Skill Required
Mic over Existing Lines	low	medium	high
Mic over Specially Placed Lines	medium	high	high
Mic Wireless	low	low	medium
Contact Microphone on Weak Spot	low	medium	medium
Hijacking Existing Microphones	low	low	high
Weakening Sound Attenuation	medium	medium	high

5.3 Electromagnetic/TEMPEST

Instead of passively capturing TEMPEST emanations from outside the SCIF perimeter, an attacker could also seek to place an antenna within the SCIF. He could then amplify the signals and thereby overpower the shielding or exfiltrate them on some other channel. He could also seek to weaken the electromagnetic shield by purposely creating holes in it or tampering with protective equipment, like power line filters.

Electromagnetic attacks are possible, but it is more likely that an attacker would place acoustic or visual sensors, which provide more direct insight into sensitive information, given the physical access necessary for these types of attacks.

Another attack is taking over devices present in the room and using their wireless capabilities to capture TEMPEST emanations. If these devices are network-connected, an attacker could exfiltrate data on their normal data connection, without having to setup an additional exfiltration path. However, similar to the insertion of bugging devices it is more likely that he will use this high level of operating system access to hijack the device's microphone or camera.

Attack Technique	Cost	Time	Technical Skill Required
Antenna + Amplification	low	medium	low
Antenna + Existing Lines	low	medium	high
Antenna + Placed Lines	medium	medium	high
Weakening Shield	medium	medium	medium
Hijack Existing Device	low	medium	high

6 Countermeasures

6.1 Physical

6.1.1 Construction Security

Later passive and active countermeasures are completely ineffective if the SCIF is breached during construction. Therefore meticulous preparation of and adherence to a Construction Security Plan (CSP) is required. The CSP covers construction personnel, site perimeter, site access, and construction materials.

6.1.1.1 Construction Personnel

Construction personnel must be vetted and monitored so that they do not pose an insider threat to the construction site and resulting facility. The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, pp. 23–27) provides for evaluation of construction workers by origin and clearance level. For example, it forbids the use of workers from SETL threat level “critical technical threat level.” Furthermore, it requires biographical data (full name, current address, Social Security Number (SSN), date and place of birth (DPOB), proof of citizenship, etc.) and fingerprint cards for background checks of all non-cleared construction personnel. It requires finish work in high-threat countries to be carried out by SECRET-cleared U.S. personnel and requires access to the site to be withdrawn if adverse security, Counterintelligence (CI), or criminal activity is detected. It also sets various requirements for the monitoring/accompanying of non-cleared workers. As an example, for new facilities it allows non-cleared workers, monitored by Construction Surveillance Technicians (CSTs) - dedicated personnel that supplement site access controls, implement screening and inspection procedures, as well as monitor construction and personnel - to perform the installation of major utilities and feeder lines. It requires that all construction personnel receive a security briefing prior to entering the site, so they know which rules to follow and what suspicious activity to report. If a construction worker leaves the project under unusual circumstances, the ICD requires the event be documented and the appropriate officer to be notified.

Not all these measures for the security vetting of construction personnel can be implemented by non-government actors. These actors should try to build a staff of long-term, trustworthy workers or employ a company that does so.

Video surveillance during the construction phase can supplement other monitoring efforts. However, it requires constant attention, just like any other non-technological security measure. Even with all the possible security mitigations and background checking, the human factor as an inside threat remains one of the most sensitive areas and the hardest to defend against.

Threats from construction personnel can also further be mitigated by careful inspection after each construction phase’s completion and [bug sweeping](#) before commissioning of the SCIF.

6.1.1.2 Site Perimeter

Without a secure perimeter, access to and within the site cannot be controlled. A secure fencing or other form of perimeter should be erected, and continuously monitored for unauthorized penetration. For renovation projects, barriers should be installed to segregate construction workers from operational activities, providing protection against unauthorized access and visual observation. When expanding SCIF space into uncontrolled areas, maximum demolition of the uncontrolled areas should be carried out beforehand. This protects against existing threats and ensures a “clean slate” before building a new SCIF. (Office of the National Counterintelligence Executive 2012, p. 25).

6.1.1.3 Site Access

Access control using badges and other forms of identification should be required entry to the site. Guards should monitor these entry points to prevent tampering and penetration attempts. Possible site control measures like identity verification, random searches, signs listing prohibited items, and vehicle inspections should be considered and weighed against the SCIF threat model. (Office of the National Counterintelligence Executive 2012, p. 27)

The IC Tech Spec also requires the use of cleared American guards (CAGs) to supervise non-U.S. and non-cleared U.S. guards, as well as to directly protect the site in high-threat, SETL category I countries. No equivalent to CAGs exists in the private sector. Their loyalty is difficult to recreate for a private actor who can’t offer the same long-term employment and ideological motivation. However, guards with a similar training level can be sourced from private suppliers and with organizational practices like supervision and vetting an adequate level of security can be ensured.

6.1.1.4 Construction Materials

Construction materials must be procured, transported, and stored in a secure way. If not, the entire security of the finished SCIF can be jeopardized by faulty or compromised materials. Inspectable materials are those that can be reasonably inspected with available measures. All other materials, as well as inspectable materials on which approved test methods were not carried out, are classified as non-inspectable and are subject to higher security requirements.

Inspectable materials can be procured from trusted suppliers without further security restrictions. Inspectable materials from non-trusted suppliers or shipped to the site in an unsecured manner should be inspected using approved methods and then moved to a secure storage area (SSA). If stored outside the SSA, a random selection of these materials should be inspected before use on the site. Non-inspectable materials should be procured from trusted suppliers or other approved channels and securely transported to the SSA. They can also be procured from untrusted suppliers if randomly chosen by trusted personnel from a suppliers shelf-stock without advance notice or indication of the intended use. No discernible purchasing patterns should be established while carrying out this randomized procurement procedure. (Office of the National Counterintelligence Executive 2012, pp. 27–29)

Secure transporation is not required for inspectable materials if they are inspected and then immediately placed in an SSA. If securely procured, shipped and stored inspectable materials may even be utilized without inspection. Non-inspectable materials, should be transported securely packaged or containerized and under the 24-hour control of an approved courier or escort officer. If this is not possible they should be securely shipped using approved transit security technical safeguards capable of detecting evidence of tampering or compromise. For government actors it may be interesting to require the transporation by military or flag carrying vessels. (Office of the National Counterintelligence Executive 2012, p. 30)

A secure storage area is a true floor to true ceiling, slab-to-slab construction of some substantial material, and a solid wood-core or steel-clad door equipped with a security lock. All inspected and securely shipped materials should be placed in the SSA immediately upon arrival and stored there until they are required for installation. Alternatively a shipping container located within a secure perimeter that is locked, alarmed, and monitored or a room or outside location enclosed by a secure perimeter that is under direct observation by cleared personnel can be used as an SSA. (Office of the National Counterintelligence Executive 2012, p. 31)

6.1.1.5 Inspection Methods

X-Ray, visual inspection, metal detectors and destructive tests can be used on inspectable materials to ensure their integrity. See (Office of the Director of National Intelligence 2020) for a detailed list of inspection methods and their uses.

6.1.1.6 Technical Security

The construction phase involves many different parties and material suppliers. It is almost impossible to defend against against down the entire supply chain. Security measures are only suitable to completely prevent the most primitive attacks and only serve to make advanced attacks more difficult. Therefore, a

technical surveillance countermeasure (TSCM) [inspection](#) should be carried out at all major construction milestones and before commissioning of the SCIF. This can effectively mitigate the impact of security breaches in the construction phase.

6.1.2 Intrusion Resistance

A secure perimeter is the foundation of a SCIF's security. Only it can prevent brute-force entries into the protected space. Without it, no other access control or locking measures are effective.

A multi-layered approach, using security in depth (SID), is most effective in ensuring a SCIF's physical security. The multiple layers can be a controlled perimeter, a secure installation, a building perimeter, an area surrounding the SCIF, and/or the SCIF Perimeter itself. If one of these layers is not existant in a sufficient degree it may be possible to supplement by beefing up one of the other layers.

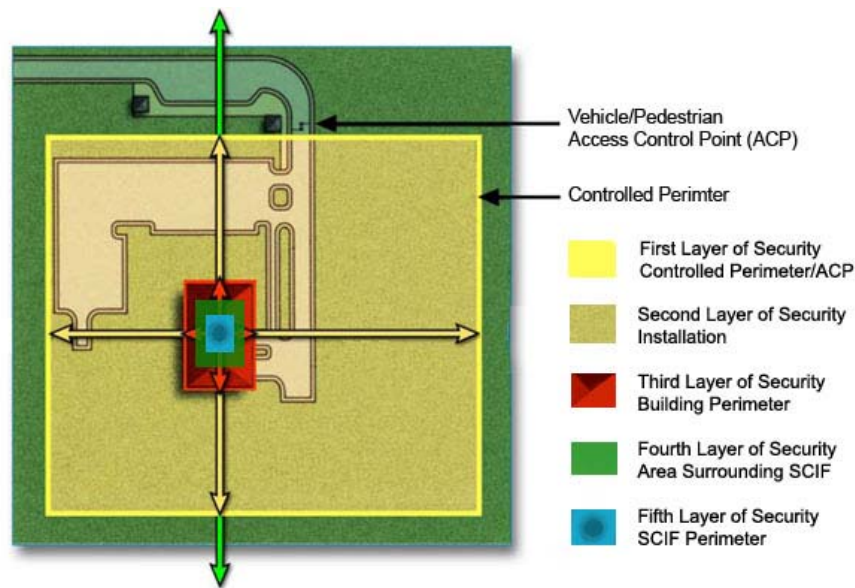


Figure 8: Map for Security in Depth of a Military Installation. Naval Facilities Engineering Systems Command Northwest (2012), p. 20

The SCIF perimeter itself should be made from a substantial material that is difficult to penetrate in a covert way. The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, pp. 8–10) proposes different wall makeups for varying mission demands. For example, an open storage facility - one in which sensitive information is stored openly and left out when not in use without further protection (Naval Facilities Engineering Systems Command

Northwest 2012, p. 16) - without SID requires a true-floor to true-ceiling wall made up of (from controlled to uncontrolled side) two 5/8" gypsum wall boards (GWB), 3/4" #9 10 gauge expanded metal spot-welded or screwed every 6" to vertical studs, 16" metal studs and runners, acoustic fill, another 5/8" GWB. Specifically the combination of multiple GWBs and expanded metal makes for a very sturdy construction. Additionally, sheet metal laminated GWB, like Knauf Diamant Steel, can be used to further enhance the resistance capabilities of the GWB. Windows are highly discouraged for security reasons (Office of the National Counterintelligence Executive 2012, p. 12).

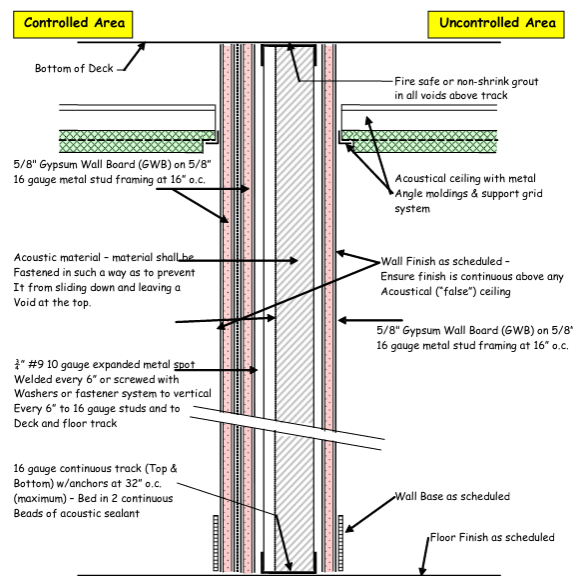


Figure 9: Wall B -Suggested Construction for Expanded Metal (Office of the National Counterintelligence Executive 2012, p. 17)

There should be only one primary entrance door to simplify personnel and visitor controlled entry. This door should be of a substantial material, like 1 3/4 inch-thick solid wood core or 1 3/4 inch-thick face steel. Its hinge pins should be located inside the SCIF perimeter or modified to prevent removal of the door, e.g., welded or set screws. (Office of the National Counterintelligence Executive 2012, pp. 11–12)

The alarm response time criteria on (Office of the National Counterintelligence Executive 2012, p. 14) requires a maximum response time of 15 minutes. Assuming that the door should resist entry for the entire alarm response time, i.e. an attacker should be captured before he breaches the door, this requirement roughly translates to DIN EN 1627 Resistance Class 5. RC 5 entails that an experienced attacker using hand tools, power tools, such as a drill, jigsaw or

reciprocating saw and an angle grinder with a max. disc diameter of 125 mm can't breach the door within 15 minutes. A SCIF door setup should meet or exceed this standard.

Closed storage of sensitive information in a security container is preferable over open storage when the SCIF is not in use. Even better, sensitive information should be stored in a separate vault when the SCIF is not in use. A security container according to the IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, p. 5) must be a General Services Administration (GSA) approved safe, which typically complies to GSA Class 6 for storage of classified information such as documents, maps, drawings, and plans (Naval Facilities Engineering Systems Command 2021). GSA Class 6 has no forced entry requirements, but requires 30 minutes resistance to covert entry and 20 hours resistance to surreptitious entry. Commercial cabinets meeting EN 14450 Grade S2 likely also fulfill the requirements of GSA Class 6.



Figure 10: Hamilton GSA Approved Class 6 4 Drawer Security Container

6.1.3 Intrusion Detection System

An intrusion detection system (IDS), also called alarm system, is essential in securing a SCIF against attackers. It allows quick detection and response to penetrations of the secured area. Multiple sensors are used in conjunction with a monitoring station to ensure round-the-clock alerts to unauthorized entry of any kind.

Mainly, the IDS is used to secure the SCIF when it is unoccupied. All interior areas through which access could be gained, including walls and doors, should be protected by IDS. Special attention should be given to detecting and responding to system outages and tampering. Limiting false alarms to a maximum of one per 30 days further ensures the reliability and effectiveness of the system, as too many false alarms cause fatigue and desensitization of security personnel. The

IDS should be stand-alone, i.e. independent of other facilities' alarm systems. It can be supplemented with [audio or video monitoring](#) if special attention is given not to inadvertently jeopardize the SCIFs information security. (Office of the National Counterintelligence Executive 2012, p. 53)

All components, i.e. the monitoring station, movement sensors, high security switches (HSS), premise control unit (PCU), and keypads should meet the internationally recognized Underwriters Laboratories (UL) Standards 2050, 639, 634, 1610 and/or 294 respectively. The UL, being an independent, international organization not complying to the standards of any one country, is most suitable for providing globally recognized and universal security standards for the purposes of this paper.

The IDS should allow for operating in access, secure, maintenance, and shunted/masked mode. Access mode is used during SCIF operation and should allow for normal entry without causing an alarm. Tampering or entry through a secondary point, like emergency exits, should continue to trigger an immediate alarm. Secure mode is used when the SCIF is unoccupied, i.e. the last person departs the SCIF. Any unauthorized entry into the SCIF should cause an alarm to be immediately transmitted to the monitoring station in secure mode. In general, there should be no remote capability to change between these modes. Maintenance mode is used during routine repairs and testing on the system. An signal for this condition should be automatically sent to the monitoring station and verified/recorded there. Generally speaking, there should be no remote access for diagnostics, maintenance or programming for security reasons. It might also become necessary to shunt/mask sensors and zones for other reasons, like unforeseen malfunctioning of specific components, however this must be displayed at the monitoring station through the period the condition exists and automatically limited in time to the next change from access to secure mode. (Office of the National Counterintelligence Executive 2012, pp. 57–58)

Electrical power supply of the IDS must be redundant, e.g. backed by 24 hours of uninterruptible power supply (UPS). On primary power failure, the IDS should be automatically transferred to emergency electrical power without causing an alarm. An indicator of the power source in use should be given at the PCU or monitoring station. (Office of the National Counterintelligence Executive 2012, p. 58)

The monitoring station must comply to UL 2050, which sets out standards for organizations monitoring, signal processing, investigating, servicing, and operating alarm systems in sensitive facilities (Convergint Technologies 2017). Governments themselves or private contractors can set up monitoring stations that meet these standards. These stations should be staffed by human operators trained in system theory and operation to effectively interpret system incidents and take appropriate response action. Any alarm event along with time of receipt, names of responding personnel, dispatch time, nature of the alarm, and follow up actions should be recorded there for at least two years. (Office of the National Counterintelligence Executive 2012, p. 59)

Sensors are the eyes and ears of an IDS. They detect breaches and trigger alarms. All sensors should be located inside the SCIF to prevent tampering and TEMPEST issues. Interior areas of a SCIF through which reasonable access could be gained should be monitored by motion sensors (UL 639) and high security switches (HSS) (UL 634 level 1 or 2). Motion sensors trigger alarms on detecting movements in their view. HSS split in two, one half mounted on moving components and the other on an adjacent rigid part. They trigger alarms when they lose internal contact between their two halves, for example when a door is opened. SCIF perimeter doors should be protected by both an HSS and a motion sensor. Failed sensors should cause continuous alarm until repaired. (Office of the National Counterintelligence Executive 2012, pp. 54–55) Seismic detectors, sensors that trigger on vibrations such as those resulting from drilling and blastic, can further be used to supplement HSS and motion sensors. There are impressive innovations in the realm of motion sensors such as passive infrared detecting attacker’s body temperature, doppler radar catching attacker’s radar reflections, cloak and camouflage detection against intruders attempting to cover their infrared signal, and anti-masking technology against attempts to obscure the field of view of the detector (Bosch Security 2021).

Premise Control Units (PCU) serve as a first point of control inside the SCIF. They as well as any associated cabling should be fully located within the SCIF perimeter. PCU should validate authorized use with an authentication technology, such as a keypad and/or card reader. Cabling between all sensors and PCU should be dedicated to the IDS and contained within SCIF. Otherwise “External Transmission Line Security” must be employed. The alarm status as well as power source in use should be continuously displayed at the PCU. A special indicator should alert to changed/failed power supply. The PCU should identify and display all activated sensors. The auto-alarm reset feature, if present, must be disabled as every security incident can only be resolved after an inspection of the SCIF and a determination for the cause of the alarm by trained personnel. Because of the sensitive nature of the information displayed, the PCU must be installed in a location that precludes observation by any unauthorized party. (Office of the National Counterintelligence Executive 2012, p. 55)

Immediate and continuous alarm must be given on any intrusion detection, failed sensor, tamper detection, or enabling of maintenance mode (maintenance message may be used in place of alarm). Alarms or maintenance messages should be displayed individually for all zones shunted or masked during maintenance mode. (Office of the National Counterintelligence Executive 2012, p. 55)

Once an IDS is set up to the above specifications, thorough acceptance testing should be carried out before the SCIF is commissioned. Motion sensors should be tested by moving at very slow speeds through the monitored area. This speed should not exceed 800 mm per second. The movements should be repeated throughout the SCIF and from different directions. The alarm must be activated at least three out of every four trials. HSS should be tested to ensure that an alarm activates before the non-hinged side of the door or window opens beyond

its own thickness from the closed position. For example, this means that the HSS triggers an alarm before the door opens 5 cm for a 5 cm door. Tamper testing should be carried out by ensuring that alarms are triggered when IDS equipment covers are opened, both in secure and access mode. These test procedures should be repeated at least semi-annually. (Office of the National Counterintelligence Executive 2012, pp. 60–61)

6.1.4 Access Control

An access control system (ACS) is employed while the SCIF is occupied to control and record personnel entry into the protected space. It is mounted in addition to the SCIF perimeter door lock to regulate access while the SCIF is in use. It does not replace this lock while the SCIF is unoccupied. (Office of the National Counterintelligence Executive 2012, p. 62)

Visual recognition of persons entering the SCIF by an authorized person at the entrance to a SCIF is the ideal access control. Should this not be possible an automated system can be used instead. (Office of the National Counterintelligence Executive 2012, p. 62)

An automated personnel ACS should use two different credentials, such as ID badge/card, PIN, and biometric identifier, to verify authorized personnel. The probability of an unauthorized individual gaining access must be no more than one in ten thousand. Card readers, keypads, communication interface devices, and other access control equipment located outside the SCIF must be tamper-protected and securely fastened to a wall or other fixed structure. Electrical components, associated wiring, or mechanical links should only be accessible from inside SCIF. Otherwise transmission lines to and from outside SCIF must be FIPS-AES certified encrypted. Equipment containing access-control software used to program in authorized persons and remove no longer authorized individuals should be located fully inside the SCIF. Electric door strikes used to unlock the door and “buzz people in” must have a positive engagement, i.e. rest in a locked position and only unlock on entry authorization. The electric door strikes should comply to UL 1034 (Burglary-Resistant Electric Locking Mechanisms). (Office of the National Counterintelligence Executive 2012, p. 63)

Records should be kept of the active assignment of ID badge/card, PIN, level of access, recent entries, and other similar system-related information. Records of personnel removed from the authorized persons list should be retained for two years. Records of security incidents should be retained for five years from the date of the incident or until the corresponding investigation is resolved. (Office of the National Counterintelligence Executive 2012, p. 63)

If the number of personnel that require access is low and there is only one entrance a non-automated access control may be used. This can consist of a mechanical, electric or electromechanical combination lock with combinations of four or more random digits. Mechanical access control devices should be

installed to prevent manipulation or access to mechanisms used for setting the access combination from outside door. For all non-automated mechanisms, the control panel or keypad should be installed to preclude unauthorized observation of combination entry or actions of combination change. The control panel with combination, cabling and wiring should be located inside the SCIF with sufficient physical security to deny unauthorized access to its mechanisms. (Office of the National Counterintelligence Executive 2012, p. 64)

6.1.5 Locks

When not occupied, SCIFs should be alarmed and secured with a FF-L-2740A compliant combination lock and a pedestrian door deadbolt meeting Federal Specification FF-L-2890 (Office of the National Counterintelligence Executive 2012, p. 11). The combination lock is used to secure the door when the SCIF is unoccupied and the access control device is used when the SCIF is occupied (Office of the National Counterintelligence Executive 2012, p. 63). The equivalent international specifications for combination locks are UL 768 and DIN EN 1300. The lowest UL 768 rating, Group 2, is essentially equivalent to FF-L-2740A (Locksmith Reference 2018).



Figure 11: Kaba X-10 Mounted Lock (FF-L-2740)

Combinations to locks installed on perimeter doors should be changed when a combination lock is first installed, when a combination has been compromised, and whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock. (Office of the National Counterintelligence Executive 2012, p. 83)

6.1.6 CCTV

Video surveillance, also known as CCTV, can be used to supplement the monitoring of SCIF entrances for the remote control of doors from within SCIF. Special attention should be given to a CCTV system to make sure that it presents no technical security hazard. (Office of the National Counterintelligence Executive 2012, p. 64). CCTV may be also used to supplement monitoring of the SCIF entrance and record events for investigation (Office of the National Counterintelligence Executive 2012, p. 75).

When CCTV is used to monitor a SCIF entrance for ACS purposes, the remote control device should be located within SCIF and should be monitored/operated by indoctrinated personnel. The cameras should provide a clear view of SCIF entrance without enabling a viewer to observe classified information when the door is open nor external control pads or access control components that would enable them to identify PINs or access procedures. The CCTV communication lines should be fully located within SCIF. Any external communication lines should be installed to prevent tampering. (Office of the National Counterintelligence Executive 2012, p. 64)

When CCTV is used to monitor a SCIF entrance for security and record-keeping purposes the system and all its components, including communications and control lines, should be exterior to SCIF perimeter. In this case it must also not enable a viewer to observe any classified information or authentication procedures.

In both cases special attention must be given that the cameras present no further technical security risk. Chinese-made video surveillance systems can be reasonably suspected of leaking information back to their Chinese State owned/controlled manufacturers (Lehman-Ludwig 2020), like HikVision and Dahua, and suffer from general bad security practices (Cyber & Infrastructure Security Agency 2017). Their use has consequently been banned from U.S. government agencies and facilities (U.S. House. 115th Congress 2018). In general, proprietary products suffer from this kind of backdoor-risk and should only be sourced from trustworthy manufacturers. Even better, they should be built in-house with [open hardware](#) components.



Figure 12: Elphel 10393 Series Free Software and Open Hardware Camera

6.2 Visual

Visual insights into the SCIF space are the easiest attack vector to defend. It suffices to create a “water-tight” outer shell without gaps or holes. Every effort should be made to exclude windows from the SCIF (Office of the National Counterintelligence Executive 2012, p. 12). If they are unavoidable they must at least be treated for visual protection, i.e. darkened with external blinds and/or laser protection film (Wolfspurger 2008, p. 463). As noted above, video surveillance systems should be designed with special attention not to provide visual insights into the space. No cameras should be installed inside the SCIF (Office of the National Counterintelligence Executive 2012, p. 82).

To protect from visual insight into the SCIF during personnel entry, entrance points should incorporate a vestibule to preclude visual observation (Office of the National Counterintelligence Executive 2012, p. 11). Double doors should have an astragal strip attached to one door to prevent observation through the door crack (Office of the National Counterintelligence Executive 2012, p. 12).

6.3 Acoustic

To secure the discussions, information processing, and conferences carried out inside the SCIF it is essential to design an effective acoustic protection system. Sound waves have the habit of finding weakpoints in even the most well-designed systems and escaping to the outside where even the faintest emission can be captured and reconstructed with digital means. Therefore, it is necessary to pay meticulous attention to detail, both in the design and build phases, while building on multiple technologies to prevent capture of usable sound information from any point.

In most cases, passive sound attenuation, walls with strong sound isolation

properties, must be combined with active sound masking, speakers that emit speech-like sounds to render useless escaping sound waves. Both out of room constraints and redundancy considerations passive sound attenuation most often doesn't suffice on its own. A sound masking system can reduce the wall thickness needed and mitigate any weakpoints that are inadvertently built into the attenuating shell.

Even protecting against attackers who manage to smuggle microphones into the SCIF space, as guests or intruders, should be considered in system design.

6.3.1 Sound Attenuation

Passive sound attenuation is the first step in reducing noise emissions from the SCIF space. Massive single-shell walls or double-shell components can be used to reduce sound transmission on all paths. Both direct transmission, sound forces on a wall to structure-borne sound in the wall to airborne sound outside the SCIF, and indirect transmission, airborne sound within the SCIF to structure-borne sound in the wall to airborne sound outside the SCIF, can be reduced with the right wall design both on primary and secondary paths. (Möser 2009, p. 253)

The sound insulation quality of building components is dependent on the frequency of the sound emission. Particularly low-frequency sound waves set walls into vibrations that they readily transmit as airborne sound to the outside. Higher frequencies are of less interest in system evaluation, because the insulation quality of walls for higher frequencies is almost always good. Problematically, the very sound emissions that need to be protected, those of the human voice, are in the low frequency range. (Möser 2009, p. 256)

A clear understanding of cut-off frequencies is essential to properly analyzing the frequency-dependent sound insulation of building components. The cut-off frequency is the frequency at which the wavelength of the airborne sound matches the length of a component's bending wave. In this frequency range, track matching occurs between the incoming airborne sound and the walls internal vibrations. They align and result in poorer airborne sound insulation. For single-shell components, sound attenuation increases with 6 dB/Octave below the cut-off frequency. This is known as Bergers' mass law. At the cut-off frequency the component's sound attenuation suffers a sharp drop and then rises with 7.5 dB/Octave. The drop is also described as the "cut-off slump" and entails significant decreases in sound attenuation at frequencies around cut-off frequency. The cut-off slump is more drastic the higher the cutoff frequency. Because of the higher sound attenuation increases above the cut-off frequency and lower cut-off slumps, it is of interest to design single-shell components with as low a cut-off frequency as possible. This can be accomplished by making the wall as rigid as possible and increasing its thickness. (Möser 2009, pp. 258–270)

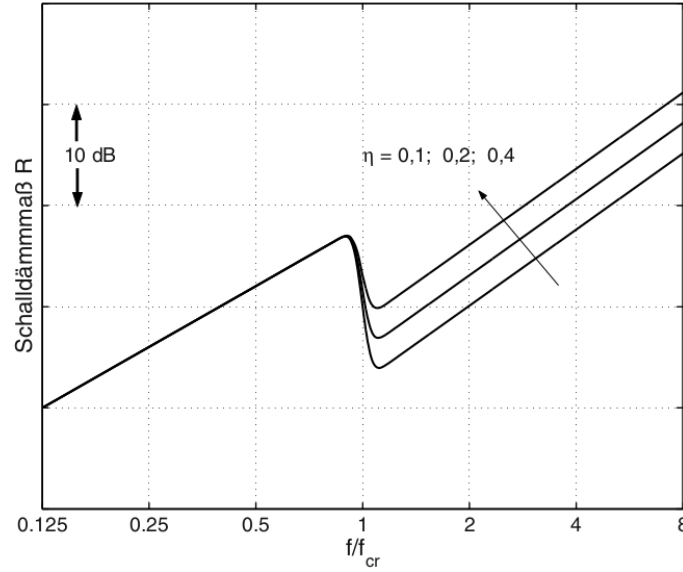


Figure 13: Principle curve of the sound reduction index frequency response of a single shell wall. η = loss factor derived from the loss mechanisms actually occurring, such as internal damping and vibration energy dissipation to adjacent components, f = frequency of emission, f_{cr} = cut-off frequency (Möser 2009, p. 267)

Increasing wall rigidity and thickness might not always be possible due to space, weight, and cost constraints. Thankfully, a better method for building attenuating walls exists, double-shell components with flexurally soft facing-shells. These make use of the propensity of the two walls to swing at different frequencies when not connected, making use of the cavity in between to create a mass-spring-mass system. No connections or cross-coupling may exist between the two shells as these destroy the spring function of the hollow space and jeopardize the entire system's effectiveness. (Möser 2009, pp. 270–276)

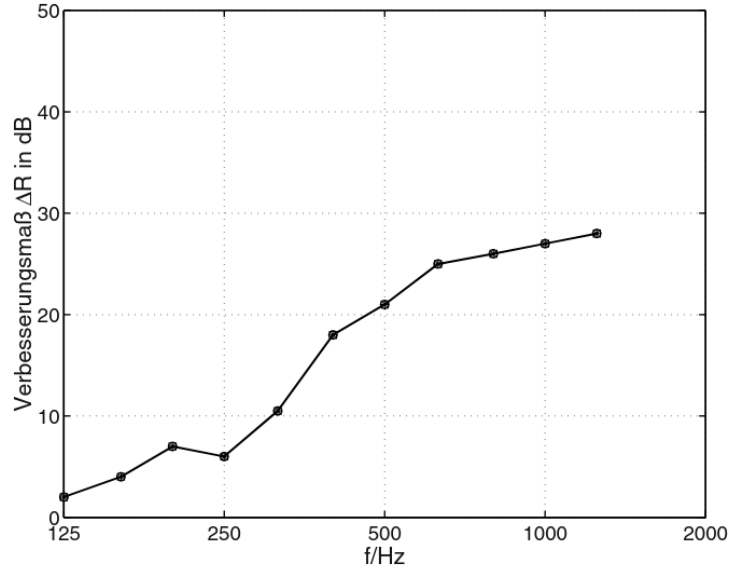


Figure 14: Improvement of the sound insulation delta R of a 80 mm plaster wall by a flexible facing shell with $m''_2 = 4 \text{ kg/m}^2$ and cavity depth $d = 65 \text{ mm}$, filled with mineral wool

Below the cut-off frequency the additional shell has no effect, however, above it the sound attenuation increases with 12 dB/octave. At the cut-off frequency there is again a slump in attenuation performance. The cut-off frequency should be engineered to be as low as possible to make use of the steep attenuation increases. According to

$$f_o \approx \frac{60 \text{ Hz}}{\sqrt{\frac{m''_2}{\text{kg/m}^2} \frac{d}{\text{m}}}}$$

a cut-off frequency of 60 Hz (well below the building acoustics frequency range beginning at 100 Hz) can be reached with a facing shell with a mass per unit area of $m''_2 = 10 \text{ kg/m}^2$ (heavy gypsum wall board) and a hollow space of $d = 10 \text{ cm}$. From here we can see that sufficiently low cut-off frequencies can be achieved without excessively heavy facing shells or massive hollow spaces. (Möser 2009, p. 273)

To achieve a high sound attenuation level it is advantageous to use heavy total masses and to distribute them unequally among the shells if possible avoiding shells of equal weight. One should also maximize the distance d between the two shells, dampen the cavity as fully as possible with absorber material, and avoid leaks or structure-borne sound bridges. (Möser 2009, p. 276)

In order to evaluate the solution on a whole system level, including floors and ceilings, one combines the walls R_W value as described in Chapter 4.2 with the longitudinal sound transmission $R_{L,w}$ of the four flanking components (two walls, ceiling, and floor) in a stepwise addition scheme specified in DIN 4109-1. The result is a total resulting sound reduction index $R'_{w,R}$ expressed in dB. (Tichelmann, Pfau 2000, p. 34)

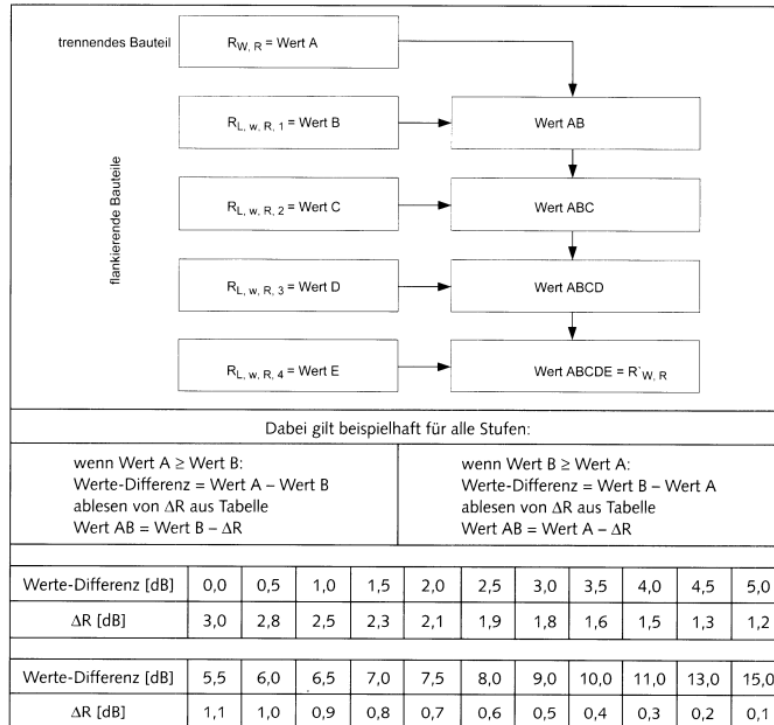


Figure 15: Stepwise addition scheme DIN 4109-1 (Tichelmann, Pfau 2000, p. 34)

Walls and flanking components aren't the only transmission paths for sound out of the SCIF. Air ducts and vents also present a significant challenge in sound attenuation. If untreated they can serve as direct transmission paths for sound waves out of the SCIF and eliminate all benefits gained from a carefully designed shell system. In order to treat air ducts and vents it is necessary to insert some type of silencer. These can be reflection mufflers, wall mufflers or active noise cancelling systems. Reflection mufflers work exclusively through reflection. Cross-section changes, branch-offs and inserted chambers reflect sound waves internally and decrease their energy. Wall mufflers Work through absorption *and* reflection. Absorbant wall lining or slim absorbant channels are used to reflect sound waves internally. Additionally, these sound waves lose energy into the mufflers absorbant surfaces. (Möser 2009, pp. 285–328)

Active noise cancelling systems produce anti-sound, amplitude inverted sound waves, to cancel out sound. They are limited in frequency range and areal effectivity. Large levels of sound reduction require very high replication accuracy in the secondary, cancelling field. (Möser 2009, pp. 405–427) Because of their complexity and relative novelty they are not the go-to solution for air vent treatment.

For reflection and wall mufflers either achieve high attenuation performance in narrow bands or moderate attenuation in wider bands. Knowing the frequency range of sound to be cancelled is essential in optimizing the mufflers. Specialized air vent mufflers for the human voice, called cross-talk sound attenuators, are readily available on the market. They achieve relatively high performance values around the frequency spectrum of the human voice and come in a box shape optimized for installation inside drywall. An off-the-shelf product from german manufacturer SHAKO KG, the cross-talk sound attenuator box AUDIX® achieves a weighted sound reduction index of R_w 38 dB at 508 mm length and 300 mm height. Normalised sound level difference, $D_{n,e}$ at the male fundamental frequency 125 Hz is 54 dB. (SCHAKO KG 2021)

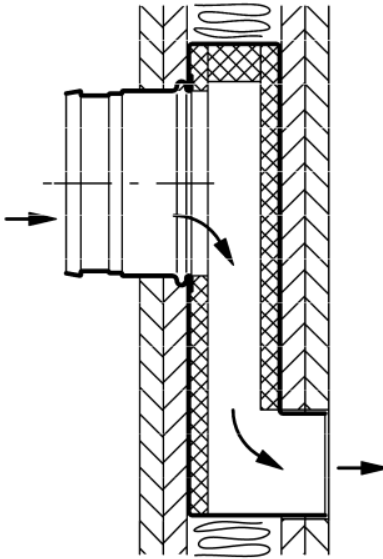


Figure 16: SCHAKO Cross-talk Sound Attenuator Box AUDIX® Installation Schematic

6.3.2 Sound Masking

When passive measures alone, out of space, weight or costs constraints, can't provide an adequate level of sound attenuation, they can be supplemented by a sound masking system. In such a system, speakers and transducers are placed

on or close to any paths that would allow audio to leave the protected space. In conjunction with a noise generator and amplifier they generate and distribute vibrations or noise that drown out escaping audio and render it useless. (Office of the National Counterintelligence Executive 2012, p. 66)

Speakers/transducers must produce sound at a higher level than the audio escaping on the path. They are placed on or close to weak points in the passive sound attenuation, like doors, windows, common perimeter walls, vents/ducts, pipes, as well as raised floors and ceilings. (Office of the National Counterintelligence Executive 2012, p. 66) For doors and windows, the transducers are placed on the frame to induce vibrations that provide a uniform audio mask and prevent contact/laser microphones from picking up usable emissions. For walls, transducers are placed at specific intervals on the studs to provide uniform protection along the entire length of the perimeter using stud-mount brackets. For vents, ducts, and pipes contact speakers are placed directly on the exterior inducing vibrations directly into the surface. In raised floors and ceilings, as well as all wall cavities, conventional dynamic cone speakers are placed in the hollow space to transmit sound through the air and induce audio interferences into adjoining parts. The speaker placement must be optimized for each room geometry and wall type. (SpeechMasking 2016)

Sound-source generators can be dedicated noise generators, tapes, discs, or digital audio players. They emit some kind of recording, music or randomly generated noise, like pink or white noise. In practice, noise sources with deterministic intensity distribution across the frequency spectrum, also called broadband noises, like pink or white noise, have been proven ineffective to mask the human voice unless used at uncomfortably loud levels (two to five times higher than the voice to be masked). They simply do not replicate the human vocal system and can be easily be filtered out by sophisticated speech extraction software. Pre-recorded sounds such as music or tracks are also easier to isolate and separate digitally from speech. Instead, it is better to use randomly generated noise from an algorithm specifically designed to imitate the spectral density, resonance, periodic pauses and interruptions, tonal and pitch qualities, and other improbable effects of human speech. (SpeechMasking 2016)

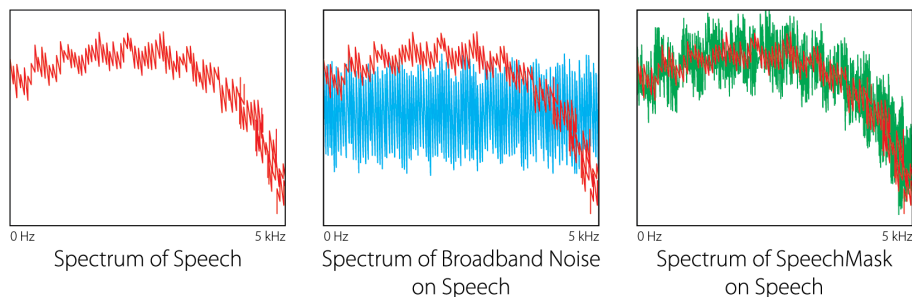


Figure 17: Comparison of broadband noise's and SpeechMask® algorithm's frequency spectrum mapped over spectrum of human speech (SpeechMasking 2016)

Even more important than the noise source itself though is the way the mask is applied and directed inside the protected space. In a properly designed system, the occupants do not hear — or only faintly hear — the mask inside the room. The only way to listen to the mask should be by listening directly against the outside wall. The intended functional area of a sound masking system is not the protected space itself but the exfiltration paths that come from it. There and only there should the sound mask present itself as vibrations and audible noise. (SpeechMasking 2016)

For security reasons, the sound masking systems should be permanently installed and not contain an AM/FM receiver. Its generators, wires and transducers should be located to the greatest extent possible within the SCIF. Generators with any capability to record ambient sound should have that capability disabled. The sound masking system should be subjected to a thorough TSCM inspection to ensure it poses no further technical risk. (Office of the National Counterintelligence Executive 2012, p. 67)

6.3.3 Microphone Jamming

Microphone jamming can play a special role in protecting the SCIF from inside attackers. A meeting participant who wishes to record the discussions without the knowledge of the other participants could smuggle in a covert recording device, like a modern smartphone. Due to their small form factor, covert recording devices often use micro-electromechanical (MEMS) microphones whose inherent hardware properties can be exploited against them to jam and render useless their recordings.

A microphone jammer makes use of the hardware non-linearity of commodity microphones. Linearity is ability to generate an electrical output proportional to the amplitude of the sound input. Any device, such as a microphone, exhibits non-linearity in some frequency bands, meaning it produces overproportional

electrical output for a given input frequency. Ultrasonic signals (centered around 25kHz) can trigger these non-linearities without being noticeable by human ears. Inside the microphone, they leak into the audible spectrum and produce jamming signals. (Chen, Li, Nagels, Li, Lopes, Zhao, Zheng 2019)

A 2019 study by University of Chicago researchers showed existing devices to be effective against smartphone microphones, but showed their inability to fully cover potential microphones at different angular positions relative to the masking device. The researchers improved upon existing devices by designing a wearable bracelet with more omni-directional speaker configuration and better angular coverage due to a user's wrist movement. (Chen, Li, Nagels, Li, Lopes, Zhao, Zheng 2019)

Existing devices are most effective against the MEMS microphones found in smartphones and other small-form factor devices. It is unclear how they perform against more sophisticated microphones designed to eliminate hardware non-linearities in the ultrasonic spectrum.

If used at all, microphone jamming systems should function supplementally to a PED policy (Office of the National Counterintelligence Executive 2012, pp. 68–72). A PED policy controls and limits the portable electronic devices allowed in the SCIF. It is especially useful when untrusted individuals are allowed entry to the SCIF to participate in discussions within.

6.4 Electromagnetic/TEMPEST Shielding

Electromagnetic shielding is used to prevent inadvertent emissions of sensitive information from the SCIF and to make information transmission from bugging devices located within it more difficult. These shields take the form of separate enclosures around the entire protected space, and make use of different physical principles to block airborne electromagnetic waves. All penetrations of the electromagnetic shield, like pipes, ducts, and cables, are treated separately to prevent the inadvertent or malicious transmission of sensitive information along them. A monitoring system can be designed to ensure the continuous performance of such a shield over time.

With the proper electromagnetic shield design, otherwise problematic signal processing equipment, like computers, can be operated inside the SCIF without concerns of leaking TEMPEST information. This saves the operator from having to block emanations at every using by using more expensive shielded equipment.

6.4.1 Functional Principles

There are multiple functional principles which electromagnetic shields can utilize to block airborne waves. Faraday cages are the simplest and most well known type of electromagnetic shields. They make use of conductive material to distribute externally induced electric charges within the conductive material cancelling the charge's effects in the cage's interior. The cage can be imagined as two metal

plates connected by an electric conductor. Because of the higher conductivity of within the material than in the surrounding air, the external field causes charges to migrate from one plate to the other instead of being wirelessly transmitted. This happens until there is no longer an electric field between the plates that could motivate charges to cross to the opposite plate. (Wolfsperger 2008, p. 90)

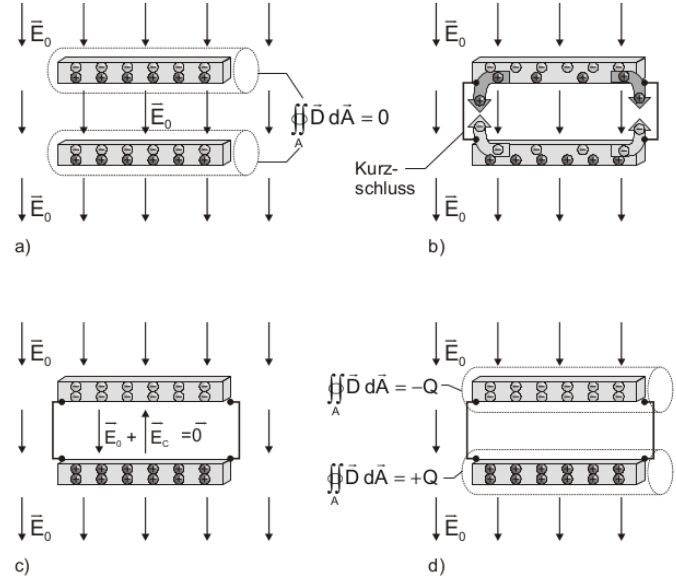


Figure 18: Two short-circuited conductive plates functioning as a Faraday cage (Wolfsperger 2008, p. 89)

Like Faraday cages, dielectric shields can be used to shield electrostatic fields. They work by refracting electric field lines at the shield's boundary. An electric field line is "bent" toward boundary when transitioning from a material with a low dielectric constant, like air, to a material with a high dielectric constant, like mineral materials. A dielectric shield must have thick walls made of a material with a high permittivity in order to achieve appreciable shielding effectiveness. For technical shields, the shielding effectiveness of dielectric shields is orders of magnitude lower than that of a Faraday cage at the same cost. Therefore, in normal cases, the shielding of electric fields is always carried out using the principle of the Faraday cage. (Wolfsperger 2008, pp. 93–94)

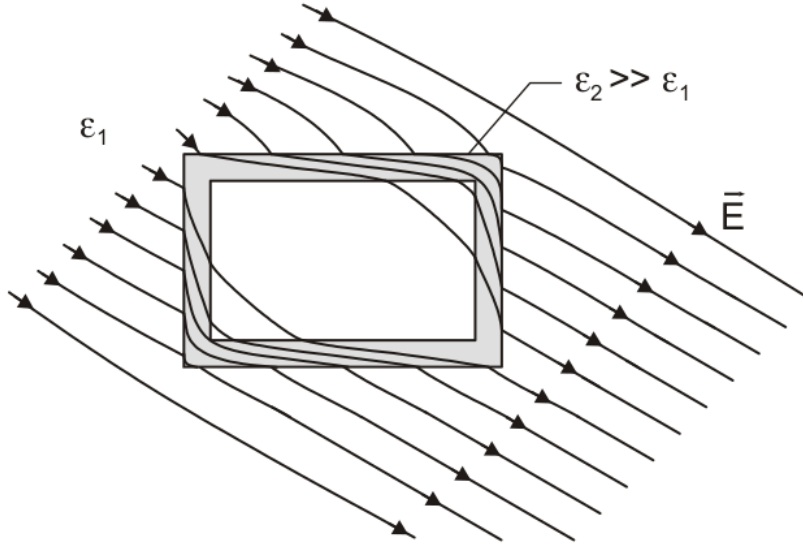


Figure 19: Dielectric screen consisting of a thick-walled sheath with a high dielectric constant (permittivity) refracting electric field lines (Wolfsperger 2008, p. 93)

Dimagnetic shields are fully analog to dielectric shields, just that they function in the realm of magnetostatic fields instead of electrostatic fields. Magnetic field lines are refracted at the boundary between materials with different magnetic permeability. The high permeability magnetostatic shield is much more important in practice than the dielectric shield. Since there is no physical effect equivalent to the Faraday cage for shielding static magnetic fields they present the only method of shielding static magnetic fields, like those emanating from electrical conductors carrying a direct current. They require high-permeability materials, such as pure iron, to provide effective shielding of both static and variable magnetic fields. [wolfsperger2008, pp. 94-96]

The most useful functional principle for the electromagnetic shielding of SCIFs is the electrodynamic shield. It shields variable magnetic fields while also functioning as a Faraday cage. Variable magnetic fields induce electric currents which in turn cause eddy currents to pile up within the conductive material. These eddy currents cause magnetic fields that are directed against the external magnetic field and cancel it out. This effect grows stronger the higher the frequency of the variable magnetic field. The electrodynamic shield must be constructed of a highly conductive material with minimal openings. Therefore it coincidentally also works as a Faraday cage. An electrodynamic shield made of an ideally conductive shell without openings shields alternating electric and variable magnetic fields as well as DC electric fields. Luckily, shielding variable

magnetic fields is of primary interest in SCIF building. Shielding against static magnetic fields is the absolute exception. (Wolfsperger 2008, pp. 100–102)

6.4.2 Materials

Electrodynamic shields are constructed from a wide variety of materials. Aluminium, steel, zinc, stainless steel, copper, brass, and tin are all useful, but come with different tradeoffs that must be evaluated when selecting an ideal material for the mission demand. The different materials with their pros and cons are listed in the table below.

Material	Pros	Cons
Aluminium	Low weight, easy to work with, high electrical conductivity	Cannot be magnetized, not so easy to weld, not as rigid as steel, electrically insulating passive corrosion layer forms on the surface (in case of joints remove the passive layer and immediately prevent new formation by applying paint or textiles)
Steel	High magnetic permeability	Corrosive
Zinc	Passive layer like aluminium	Low nobility (contact with metals higher on the galvanic series problematic for corrosion)
Stainless steel	Relatively good electrical conductivity, high corrosion resistance (preferred material for electrodynamic shields)	High price, high weight, difficult processing with cutting tools, poor shielding of low frequency fields due to low permeability
Copper	No interfering protective oxidation layers, soft, easy soldering	Very high price
Brass	Good corrosion resistance, harder than copper	Low conductivity, very expensive

Material	Pros	Cons
Tin	Useful as alloy or corrosion protection	Too soft

For electrodynamic shields, the conductivity of the material is most important. Permeability and dielectricity are secondary. The material must be installed with a minimum thickness, which can be derived mathematically from the penetration depth of the given frequency in the material. The greater the wall clearance between the perimeter walls, the higher the shielding effect. Homogeneous screens, those made of only one material, the performance of larger shields exceed those of smaller shields, because penetrating energy can be better distributed over a larger volume. As an example, 100 dB shielding effectiveness can be reached for a stainless steel shield with 1 m wall clearance and 2 mm thickness at the lowest generally usable radio frequency, 100 kHz. (Wolfsperger 2008, pp. 227–247)



Figure 20: Electrodynamic shield in the offices of finnish IT security firm F-Secure (Leyden 2015)

The continuously electrically conductive connection of shielding materials is of utmost importance for the effectivity of the entire shield. Gaps of even half a wavelength in size can nullify the entire shield. Many materials have the propensity to build passive oxidation layers that protect them from further corrosion. These must be carefully removed when joining such materials in order to ensure electric conductivity. These stripped surfaces, as well as corrosive

materials not covered by a passive layer, must be immediately covered by a protective coating upon installation as a component of the shield. This prevents the regeneration of the non-conductive passive layer or further corrosion in the case of corrosive materials. Another factor in the joining of materials, specifically materials with different electrode potential, is contact corrosion. When materials on opposite ends of the galvanic series are joined they can build a cathode-anode pair that results in the decay of both materials over time. (Wolfsperger 2008, pp. 249–252)

6.4.3 Joints and Gaskets

The ideal methods for joining components ensuring consistently high, “watertight” conductivity are soldering and welding. Riveting or screwing are also effective as long as the distances are small compared to the relevant minimum wavelength. However, these ideal methods are not applicable to connections that need to be opened and closed over time, for example those found in a door. For such joints, there are different types of HF (high frequency) gaskets that can provide fully electrically conductive connections over long periods of use. (Wolfsperger 2008, pp. 252–253)

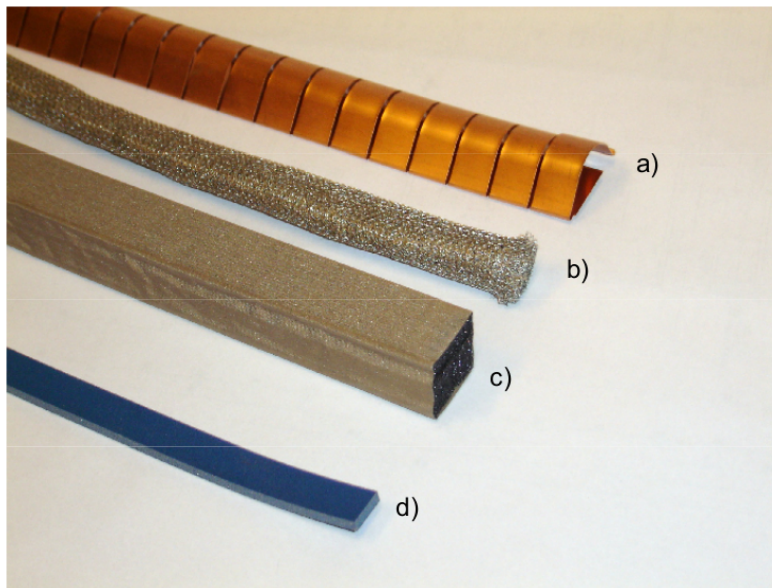


Figure 21: Different types of gaskets a) Contact feather, b) Wire mesh c) Elastomer gasket with conductive textile coating d) Conductive elastomer gasket (Wolfsperger 2008, p. 267)

Contact feathers consist of stainless steel or copper beryllium, a highly elastic copper alloy, which is pressed against a conductive surface when the moving

part is closed. The contact pressure enables excellent contact properties with low electrical resistance over long periods of time and many closing cycles. Contact feathers are self-cleaning, when pressing the contact springs against the conductive surface, the spring grinds over the metal surface and removes any oxide layers or small dirt on both surfaces. On the other hand, they are highly susceptible to mechanical damage, require high contact pressure, have a low tolerance for deviating gap dimensions, offer no insulation against outside air, and come with a high price. (Wolfsperger 2008, pp. 254–258)

Wire mesh gaskets are made up of a stainless steel, copper beryllium, aluminum or monel, an alloy of approximately 65% nickel, 33% copper and 2% iron, mesh that is pressed against a conductive surface when the component is closed. They have good contact properties with low electrical resistance over long periods of times. They are very robust featuring low susceptibility to mechanical damage. Any passive oxidation layers are broken through by the individual wires when the contact pressure is applied. However, they also require very high contact pressures, have a low tolerance for deviating gap dimensions, offer no insulation against outside air, and come at a high price point. Furthermore, they have weaker self cleaning properties than contact feathers and require contact pressure to always be applied perpendicular to the gasket. (Wolfsperger 2008, pp. 258–261)

Elastomer gaskets, both those consisting entirely of conductive material and those only covered by conductive textile, have generally weaker shielding properties than the above two gasket types. They sit between the moving part and its frame. Due to their elastic properties they are compressed by the closure and act as a conductor between them. They require lower contact pressures than contact feathers or wire mesh gaskets, have a higher tolerance for deviating gap dimensions, are very resistant to mechanical damage, insulate against outside air, and come at a very low price point. However, they do not have self-cleaning properties, don't counteract passive oxidation layers, and are less durable over time. (Wolfsperger 2008, pp. 261–267)

It is the designers job to weigh the different gaskets' strengths and weaknesses and select the ideal type for the individual SCIF and component.

6.4.4 Penetrations

Electrical lines, data connections and control cables must all pass through the electromagnetic shield without degrading the shields performance or losing connection quality. HVAC vents/ducts and in some cases water pipes must carry utilities in and out of the SCIF without degrading shielding performance or affecting throughput to an excessive degree. Screws for lights and other fixtures must also puncture the shielding without reducing its performance. All these different challenges require individual solutions that must be incorporated in the design from the outset.

Electrical power lines should pass into the SCIF through a power line filter. This filter only allows the 50 Hz frequency of the power grid to pass through while

“filtering” out all other transmissions. Their enclosure should be mounted to the wall shielding in order to make its shielding continuous with that of the room. Similar filters also exist for control lines. (Wolfsperger 2008, pp. 271–276)

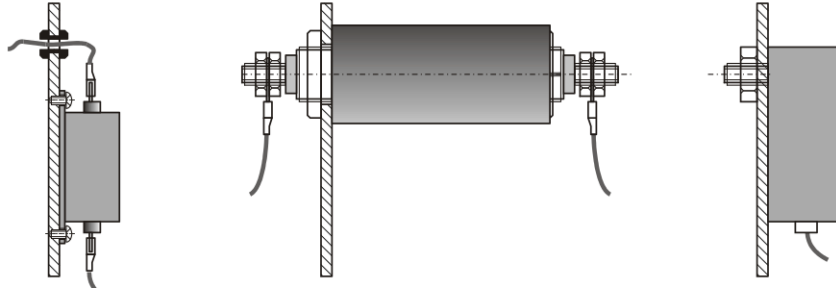


Figure 22: Different mounting configurations of power line filters (Wolfsperger 2008, p. 276)

Data lines are best passed through the electromagnetic shield by converting them to fiber optic cables using a media converter. Fiber optic cables not only enable very high data transmission rates, but they are also beneficial from a shielding perspective, since they are made entirely from non-conductive material. To eliminate electromagnetic leaks through the cable tunnel, they should be fed through hollow conductors whose cut-off frequency is sufficiently high or through special fiber optic grommets. The purpose-built grommets wrap tightly around the individual fiber optic cores leaving no gaps for even the highest-frequency leaking emanations. (Wolfsperger 2008, p. 281)

Heating, ventilation, and air conditioning vents and ducts should incorporate honey comb panels at the protected space boundary. These make use of the fact that hollow conductors have high attenuation properties below their cut-off frequency. With sufficiently small hollow conductors the cut-off frequency can be raised to a point that almost all waves fall in this highly attenuating spectrum below the cut-off frequency. (Wolfsperger 2008, pp. 282–284) Due to their small hollow spaces honeycomb filters restrict air flow. They must be dimensioned with a sufficiently large cross-section area to supply the necessary air for all occupants and discharge an equivalent amount of exhaust air. Ventilation is absolutely necessary in SCIFs with airtight electromagnetic shields, otherwise there is a serious risk of suffocation for the occupants. As an example, a SCIF with 10 occupants requires ca. $360 \text{ m}^3/\text{h}$ of fresh air per hour. With a ventilation duct with a cross-section area of 0.1 m^2 ($30 \times 30 \text{ cm}$) this results in a necessary air flow velocity of $3600 \text{ m/h} = 1 \text{ m/s}$. Under these conditions, a 18 GHz honeycomb panel would cause a pressure loss of 0.1 mbar which would have to be compensated by the ventilation system. The same goes for the exhaust air side. (Wolfsperger 2008, pp. 355–358)

Refrigerant lines and water pipes should be fed through purpose-built pipe penetrations as shown in Wolfsperger (2008) Schematic 4.40 and 4.52. These enclose the tubes or pipes and ensure electrical conductivity around the circumference of the penetration.

Designated heating and cooling of the room can be achieved using electrical heating fed through the line filter and a ductless minisplit units with all refrigerant and control lines fed through the shielding as described above.

A vapor barrier should be installed on both sides of the perimeter wall to protect it from moisture penetration by condensate. Especially with a mobile SCIF unit, the vapor pressure gradient can alternate throughout the year. Sometimes transpiration and heating on the inside with simultaneous cold air conditions on the outside will cause moisture to diffuse from the inside to the outside, while AC on the inside with high temperatures and humidity on the outside (tropical conditions) will cause moisture to diffuse in the other direction. The wall should be protected from both cases. (Wolfsperger 2008, pp. 358–360)

6.4.5 Safety

A shielded room must never be operated without proper grounding. Otherwise, the leaking currents from the power line filters can flow to the electrical ground in an undefined manner via the high-impedance connections between the power line filter and the shield itself. This would result in the entire line voltage being fed onto the SCIF perimeter walls, presenting a potential danger to the life of the personnel working within the SCIF. A shielded room or area should only be grounded at a single point so that no equalizing currents (usually magnetically induced) can flow through the shielding. In addition, a residual current circuit breaker should be installed to protect occupants from ongoing electric shocks.

6.4.6 Shielding System Function Monitoring

In his book, Hans Wolfsperger also proposes a system to continuously monitor the function of the room shielding during use. He proposes that the RF output of a spectrum analyzer be fed through an amplifier to a broadband transmitting antenna permanently installed in the room. A receiving antenna, e.g. a leak detector, would also be permanently installed on the outside of the room and connected to the input of the spectrum analyzer. During the first functional tests, when the system is determined to be effective, the spectrum analyzer would determine and store the frequency response of the shielded transmission. Each time the shielding is checked, the frequency spectrum would be determined again and compared with the stored values. If clear deviation from the reference are detected, the shielding would have to be checked for errors. (Wolfsperger 2008, pp. 466–467)

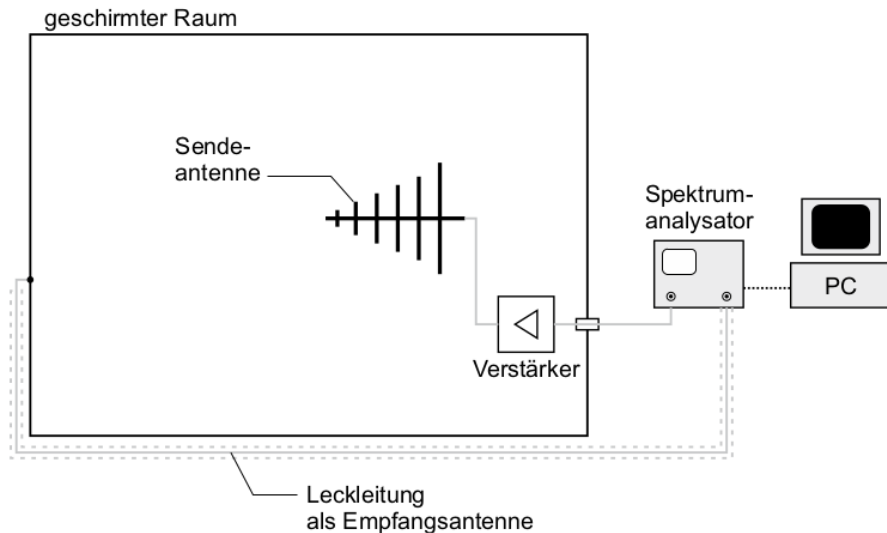


Figure 23: Shield monitoring system schematic (Wolfsperger 2008, p. 467)

This system could help mitigate against sabotage and performance losses over time, which would otherwise only be detected by periodic shield attenuation measurements. Because of their high equipment and personnel costs these are conventionally only conducted annually, if at all. Undetected leaks can therefore persist for long time periods and nullify the large effort that went into the planning and construction of the shield in the first place. Such a system is not yet commercially available and would have to be specially planned and implemented. (Wolfsperger 2008, pp. 466–467)

6.4.7 Signal Jamming

Signal jamming cannot be used as an equivalent to sound masking in electromagnetic shielding. Signal jamming works by deliberately transmitting signals on the same radio frequencies as mobile phones and other wireless devices, disrupting the communication between the devices and their base stations, effectively disabling them within the range of the jammer.

It is not possible to closely target these disruptive transmissions, as with sound masking, so they can interfere with the legitimate functioning of devices inside the SCIF and surround it. Because of this, they are illegal in the EU under Directive 1999/5/EC and in the US under the Communications Act of 1934.

6.5 Bug Sweeping

7 Example Module

This section will propose an example solution for a Sensitive Compartmented Information Facility (SCIF). It will employ the above passive and active countermeasures in a shipping container sized ($\sim 6 \times 2.4 \times 2.7$ m) module to reach the quantitative limits on information source leaks defined above.

7.1 Physical

7.2 Visual

7.3 Sound

7.4 Electromagnetic/TEMPEST

References

BOSCH SECURITY, 2021. *Commercial Series TriTech AM Motion Detectors with Anti-mask*. March 2021. https://resources-boschsecurity-cdn.azureedge.net/public/documents/Commercial_Series_Tr_Data_sheet_enUS_75201763083.pdf.

CHEN, Yuxin, LI, Huiying, NAGELS, Steven, LI, Zhijing, LOPES, Pedro, ZHAO, Ben Y. and ZHENG, Haitao, 2019. Understanding the Effectiveness of Ultrasonic Microphone Jammer. *CoRR* [online]. 2019. Vol. abs/1904.08490. Available from: <http://arxiv.org/abs/1904.08490>

CONVERGINT TECHNOLOGIES, 2017. *Meet UL 2050 Standards for Closed Rooms and SCIFs*. September 2017. <https://www.convergent.com/meet-ul-2050-standards-for-closed-rooms-and-scifs/>.

CYBER & INFRASTRUCTURE SECURITY AGENCY, 2017. *Hikvision Cameras* [online]. May 2017. ICS Advisory (ICSA-17-124-01). Available from: <https://us-cert.cisa.gov/ics/advisories/ICSA-17-124-01>

DEUTSCHES INSTITUT FÜR NORMUNG, 2018. DIN 4109-1:2018-01: *Sound Insulation in Buildings - Part 1: Minimum Requirements*. Berlin: Beuth Verlag.

EMCTEST TECHNOLOGIES, 2018. *NSA 94-106 Effectiveness Testing RF Shielded Enclosures*. 2018. <https://www.shieldingtests.com/?standard=NSA-94-106>.

GENKIN, Daniel, PACHMANOV, Lev, PIPMAN, Itamar and TROMER, Eran, 2015. Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. *Tel Aviv University*. February 2015.

GÖSELE, K. and SCHRÖDER, E., 2004. Schalldämmung in Gebäuden. In: *Taschenbuch der Technischen Akustik*. Berlin, Heidelberg: Springer-Verlag.

KRIEGER PRODUCTS, 2015. *Radio Frequency Interference (RFI) Shielding Principles*. 2015. <https://www.kriegerproducts.com/downloads/general/RFI-Shielding-Principles.pdf>.

LEHMAN-LUDWIG, Anna, 2020. *Hikvision, Corporate Governance, and the Risks of Chinese Technology*. August 2020. <https://www.csis.org/blogs/technology-policy-blog/hikvision-corporate-governance-and-risks-chinese-technology>.

LEYDEN, John, 2015. Old tech, new battles: Inside F-Secure's formidable Faraday cage. *The Register* [online]. November 2015. Available from: https://www.theregister.com/2015/11/11/f_secure_lab_tour_faraday_cage/

LIU, Zhuoran, SAMWEL, Niels, WEISSBART, Léo, ZHAO, Zhengyu, LAURET, Dirk, BATINA, Lejla and LARSON, Martha, 2020. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *Radboud University*. November 2020.

LOCKSMITH REFERENCE, 2018. *Ratings for Safe Locks*. October 2018. <https://lockreference.com/ratings-for-safe-locks/>.

MÖSER, Michael, 2009. *Technische Akustik*. Berlin, Heidelberg: Springer-Verlag.

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND, 2021. *Introduction to GSA-approved Security Containers*. January 2021. https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock/SecurityHardware/SecurityContainers.html.

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND NORTHWEST, 2012. *Physical Security of Sensitive Compartmented Information Facilities (SCIF)*. November 2012. https://www.washingtonpost.com/news/politics/wp-content/uploads/sites/11/2017/02/navfac_scif_ho.pdf.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2020. *Inspectable Construction Materials Checklist*. July 2020. <https://www.dni.gov/files/Governance/Inspectable-Materials-Checklist-V15.pdf>.

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, 2012. *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities Version 1.2 - IC Tech Spec-for ICD/ICS 705*. 2012. <https://fas.org/irp/dni/icd/ics-705-ts.pdf>.

RTL-SDR.COM, 2017. *TempestSDR: An SDR tool for Eavesdropping on Computer Screens via Unintentionally Radiated RF*. November 2017. <https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/>.

SCHAKO KG, 2021. *Technical Documentation for Cross-talk Sound Attenuator Box AUDIX®*. March 2021. https://schako.com/wp-content/uploads/audix_en.pdf.

- SPEECHMASKING, 2016. *Industry-Leading Speech Privacy*. 2016. <https://www.speechmasking.com>.
- TICHELMANN, Karsten and PFAU, Jochen, 2000. *Entwicklungswandel Wohnungsbau: Neue Gebäudekonzepte in Trocken- und Leichtbauweise*. Wiesbaden: Vieweg+Teubner Verlag.
- U.S. HOUSE. 115TH CONGRESS, 2018. *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. August 2018. H.R.5515.
- U.S. NATIONAL SECURITY AGENCY, 1972. *TEMPEST: A Signal Problem*. 1972. <http://www.jproc.ca/crypto/tempest.pdf>.
- U.S. NATIONAL SECURITY AGENCY, 1994. *NSA 94-106 National Security Agency Specification for Shielded Enclosures*. 1994. <http://cryptome.info/0001/nsa-94-106.htm>.
- WOLFSPERGER, Hans A., 2008. *Elektromagnetische Schirmung: Theorie und Praxisbeispiele*. Berlin, Heidelberg: Springer-Verlag.